



FortiMail 5.4.0 CLI Reference



FortiMail 5.4.0 CLI Reference

August 18, 2017

2nd Edition

Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of contents

Using the CLI	8
Connecting to the CLI	8
Command syntax.....	13
Sub-commands	16
Permissions	19
Tips and tricks	23
config.....	27
antispam behavior-analysis	28
antispam bounce-verification key.....	29
antispam deepheader-analysis.....	30
antispam endpoint reputation blacklist.....	30
antispam endpoint reputation exempt.....	31
antispam greylist exempt.....	31
antispam quarantine-report	33
antispam settings.....	34
antispam trusted	44
archive account	45
archive exempt-policy	48
archive journal.....	49
archive policy.....	49
customized-message.....	50
dlp scan-rules	78
domain	79
domain-association	133
file filter.....	133
file signature.....	134
log setting remote	134
log setting local.....	137
log alertemail recipient.....	139
log alertemail setting.....	140
mailsetting host-mapping	141
mailsetting mail-scan-options.....	142
mailsetting preference	143
mailsetting proxy-smtp	144
mailsetting relay-host-list.....	145
mailsetting sender-email-addr-handling.....	146

mailsetting smtp-rcpt-verification	147
mailsetting storage central-ibe	147
mailsetting storage central-quarantine	148
mailsetting storage config.....	150
mailsetting systemquarantine	151
policy access-control receive	152
policy access-control delivery	158
policy ip.....	160
policy recipient.....	163
profile antispam	166
profile antispam-action	172
profile antivirus.....	176
profile antivirus-action	179
profile authentication	183
profile certificate-binding	187
profile content.....	188
profile content-action.....	198
profile dictionary	203
profile dictionary-group	208
profile email-address-group	208
profile encryption	209
profile ip-address-group	210
profile ip-pool.....	211
profile ldap	211
profile notification	226
profile resource	227
profile session	229
profile tls	243
report	244
sensitive data	246
system accprofile.....	248
system admin.....	249
system appearance	251
system backup-restore-mail.....	253
system central-management	255
system certificate ca.....	256
system certificate crl.....	256
system certificate local	257
system certificate remote	258
system ddns	258

system disclaimer	260
system disclaimer-exclude	261
system dns.....	262
system encryption ibe.....	263
system encryption ibe-auth	266
system fortiguard antivirus	267
system fortiguard antispam	269
system fortisandbox	270
system global.....	273
system ha.....	276
system interface.....	285
system mailserver	291
system password-policy	297
system port-forwarding	298
system route	299
system saml.....	300
system scheduled-backup	300
system security authserver	300
system snmp community.....	301
system snmp sysinfo	303
system snmp threshold	303
system snmp user.....	304
system time manual.....	306
system time ntp	307
system webmail-language	308
system wccp settings	309
user alias	309
user map	310
user pki	313
execute	316
backup	317
backup-restore	318
certificate	319
checklogdisk.....	321
checkmaildisk	322
cleanqueue	322
create	322
date	324
db.....	325
dlp.....	326

endpoint.....	326
erase filesystem	326
factoryreset	327
factoryreset disk	327
fips	328
formatlogdisk	329
formatmaildisk	329
formatmaildisk_backup.....	330
forticloud	331
ha commands	331
license	332
ibe data	332
ibe user	332
lvm	333
maintain	333
nslookup	334
partitionlogdisk	336
ping	337
ping-option	338
ping6	339
ping6-option	340
raid	341
reboot.....	342
reload	342
restore as	343
restore av	343
restore config.....	344
restore image	346
restore mail-queues	347
sched-backup	347
shutdown	347
smtpptest	348
ssh	349
storage	349
telnettest	350
traceroute.....	350
update	352
user-config.....	352
vm	352

get	354
system performance	354
system status.....	355
show & show full-configuration	357
Index	359

Using the CLI

The command line interface (CLI) is an alternative to the web user interface (web UI).

Both can be used to configure the FortiMail unit. However, to perform the configuration, in the web UI, you would use buttons, icons, and forms, while, in the CLI, you would either type lines of text that are commands, or upload batches of commands from a text file, like a configuration script.

If you are new to Fortinet products, or if you are new to the CLI, this section can help you to become familiar.

This section contains the following topics:

- [Connecting to the CLI](#)
- [Command syntax](#)
- [Sub-commands](#)
- [Permissions](#)
- [Tips and tricks](#)

Connecting to the CLI

You can access the CLI in two ways:

- **Locally** — Connect your computer directly to the FortiMail unit's console port.
- **Through the network** — Connect your computer through any network attached to one of the FortiMail unit's network ports. The network interface must have enabled Telnet or SSH administrative access.

Local access is required in some cases.

- If you are installing your FortiMail unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection. See the *FortiMail Install Guide*.
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process has completed, and therefore local CLI access is the only viable option.

Before you can access the CLI through the network, you usually must enable SSH and/or Telnet on the network interface through which you will access the CLI.

This section includes:

- [Connecting to the CLI using a local console](#)
- [Enabling access to the CLI through the network \(SSH or Telnet\)](#)
- [Connecting to the CLI using SSH](#)
- [Connecting to the CLI using Telnet](#)

Connecting to the CLI using a local console

Local console connections to the CLI are formed by directly connecting your management computer or console to the FortiMail unit, using its DB-9 or RJ-45 console port.

Requirements

- a computer with an available serial communications (COM) port
- the RJ-45-to-DB-9 or null modem cable included in your FortiMail package
- terminal emulation software such as [PuTTY](#)



The following procedure describes connection using PuTTY software; steps may vary with other terminal emulators.

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiMail unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start PuTTY.
3. In the *Category* tree on the left, go to *Connection* > *Serial* and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None

4. In the *Category* tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
5. Click *Open*.
6. Press the Enter key to initiate a connection.
The login prompt appears.
7. Type a valid administrator account name (such as `admin`) and press Enter.
8. Type the password for that administrator account then press Enter. (In its default state, there is no password for the `admin` account.)

The CLI displays the following text, followed by a command line prompt:

```
Welcome!
```

You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see “[Enabling access to the CLI through the network \(SSH or Telnet\)](#)” on page 9.

Enabling access to the CLI through the network (SSH or Telnet)

SSH or Telnet access to the CLI requires connecting your computer to the FortiMail unit using one of its RJ-45 network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is **not** connected directly or through a switch, you must also configure the FortiMail unit with a static route to a router that can forward packets from the FortiMail unit to your computer.

You can do this using either:

- a local console connection (see the following procedure)
- the web-based manager (see the [FortiMail Install Guide](#) or [FortiMail Administration Guide](#))

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as [PuTTY](#)
- the RJ-45-to-DB-9 or null modem cable included in your FortiMail package
- a network cable
- prior configuration of the operating mode, network interface, and static route (for details, see the [FortiMail Install Guide](#))

To enable SSH or Telnet access to the CLI using a local console connection

1. Using the network cable, connect the FortiMail unit's network port either directly to your computer's network port, or to a network through which your computer can reach the FortiMail unit.
2. Note the number of the physical network port.
3. Using a local console connection, connect and log into the CLI. For details, see "[Connecting to the CLI using a local console](#)" on page 8.
4. Enter the following commands:

```
config system interface
  edit <interface_name>
    set allowaccess {http https ping snmp ssh telnet}
  end
```

where:

- <interface_str> is the name of the network interface associated with the physical network port, such as port1
- {aggregator http https ping ssh telnet webservice} is the complete, space-delimited list of permitted administrative access protocols, such as https ssh telnet; omit protocols that you do not want to permit

For example, to exclude HTTP, SNMP, and Telnet, and allow only HTTPS, ICMP ECHO (ping), and SSH administrative access on port1:

```
config system interface
  edit "port1"
    set allowaccess ping https ssh
  next
end
```



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

5. To confirm the configuration, enter the command to view the access settings for the interface.

```
show system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the interface.

To connect to the CLI through the network interface, see [“Connecting to the CLI using SSH” on page 11](#) or [“Connecting to the CLI using Telnet” on page 12](#).

Connecting to the CLI using SSH

Once the FortiMail unit is configured to accept SSH connections, you can use an SSH client on your management computer to connect to the CLI.

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths vary by whether or not you have enabled FIPS-CC mode, but generally include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a FortiMail network interface configured to accept SSH connections (see [“Enabling access to the CLI through the network \(SSH or Telnet\)” on page 9](#))
- terminal emulation software such as PuTTY

To connect to the CLI using SSH

1. On your management computer, start PuTTY.
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.
3. In *Port*, type 22.
4. From *Connection type*, select SSH.
5. Click *Open*.

The SSH client connects to the FortiMail unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiMail unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiMail unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiMail unit with no network hosts between them, this is normal.

6. Click Yes to verify the fingerprint and accept the FortiMail unit’s SSH key. You will not be able to log in until you have accepted the key.

The CLI displays a login prompt.

7. Type a valid administrator account name (such as `admin`) and press Enter.



You can alternatively log in using an SSH key. For details, see [“system admin” on page 249](#).

8. Type the password for this administrator account and press Enter.



If four incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The CLI displays a command line prompt (by default, its host name followed by a #). You can now enter CLI commands.

Connecting to the CLI using Telnet

Once the FortiMail unit is configured to accept Telnet connections, you can use a Telnet client on your management computer to connect to the CLI.



Telnet is not a secure access method. SSH should be used to access the CLI from the Internet or any other untrusted network.

Requirements

- a FortiMail network interface configured to accept Telnet connections (see [“Enabling access to the CLI through the network \(SSH or Telnet\)”](#) on page 9)
- terminal emulation software such as PuTTY

To connect to the CLI using Telnet

1. On your management computer, start PuTTY.
2. In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled Telnet administrative access.
3. In *Port*, type 23.
4. From *Connection type*, select *Telnet*.
5. Click *Open*.
The CLI displays a login prompt.
6. Type a valid administrator account name (such as `admin`) and press Enter.
7. Type the password for this administrator account and press Enter.



If three incorrect login or password attempts occur in a row, you will be disconnected. Wait one minute, then reconnect to attempt the login again.

The CLI displays a command line prompt (by default, its host name followed by a #). You can now enter CLI commands.

Logging out from the CLI console

No matter how you connect to the FortiMail CLI console (direct console connection, SSH, or Telnet), to exit the console, enter the *Exit* command.

Command syntax

When entering a command, the command line interface (CLI) requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

Fortinet documentation uses the following conventions to describe valid command syntax.

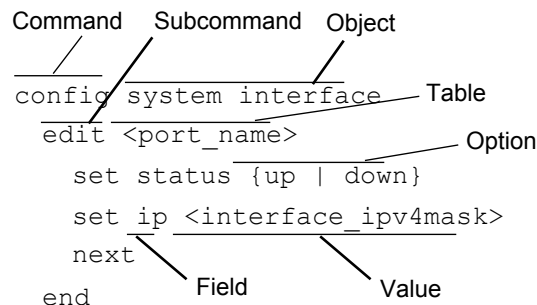
Terminology

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

To describe the function of each word in the command line, especially if that nature has changed between firmware versions, Fortinet uses terms with the following definitions.

Figure 1: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiMail unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line.

Valid command lines must be unambiguous if abbreviated. (See [“Command abbreviation” on page 24.](#)) Optional words or other command line permutations are indicated by syntax notation. (See [“Notation” on page 14.](#))



This CLI Reference is organized alphabetically by object for the `config` command, and by the name of the command for remaining top-level commands.

- **sub-command** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands. (See [“Indentation” on page 14.](#))

Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope. (See [“Sub-commands” on page 16.](#))

- **object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or

numbered sets are sometimes referenced by other parts of the configuration that use them. (See “[Notation](#)” on page 14.)

- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiMail unit will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See “[Notation](#)” on page 14.)
- **option** — A kind of value that must be one or more words from of a fixed set of options. (See “[Notation](#)” on page 14.)

Indentation

Indentation indicates levels of nested commands, which indicate what other sub-commands are available from within the scope.

For example, the `edit` sub-command is available only within a command that affects tables, and the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  next
end
```

For information about available sub-commands, see “[Sub-commands](#)” on page 16.

Notation

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 1: Command syntax notation

Convention	Description
Square brackets []	A non-required word or series of words. For example: <code>[verbose {1 2 3}]</code> indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: <code>verbose 3</code>

Table 1: Command syntax notation

<p>Angle brackets < ></p>	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example:</p> <pre><retries_int></pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> • <xxx_name>: A name referring to another part of the configuration, such as <code>policy_A</code>. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <xxx_email>: An email address, such as <code>admin@mail.example.com</code>. • <xxx_url>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet./com/</code>. • <xxx_ipv4>: An IPv4 address, such as <code>192.168.1.99</code>. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <xxx_ipv4range>: A hyphen (-)-delimited inclusive range of IPv4 addresses, such as <code>192.168.1.1-192.168.1.255</code>. • <xxx_ipv6>: A colon (:)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. • <xxx_v6mask>: An IPv6 netmask, such as <code>/96</code>. • <xxx_ipv6mask>: An IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is <i>not</i> another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See "Special characters" on page 24. • <xxx_int>: An integer number that is <i>not</i> another data type, such as 15 for the number of minutes.
<p>Curly braces { }</p>	<p>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces.</p> <p>You must enter at least one of the options, unless the set of options is surrounded by square brackets [].</p>

Table 1: Command syntax notation

Options delimited by vertical bars 	Mutually exclusive options. For example: <code>{enable disable}</code> indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: <code>{http https ping snmp ssh telnet}</code> indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code> Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Sub-commands

Once you have connected to the CLI, you can enter commands.

Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

Sub-commands are available from within the scope of some commands. When you enter a sub-command level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin) #
```

Applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command.

For example, the `edit` sub-command is available only within a command that affects tables; the `next` sub-command is available only from within the `edit` sub-command:

```
config system interface
  edit port1
    set status up
  next
end
```



Sub-command scope is indicated in this CLI Reference by indentation. See [“Indentation” on page 14](#).

Available sub-commands vary by command. From a command prompt within `config`, two types of sub-commands might become available:

- commands affecting fields
- commands affecting tables



Syntax examples for each top-level command in this CLI Reference do not show all available sub-commands. However, when nested scope is demonstrated, you should assume that sub-commands applicable for that level of scope are available.

Table 2: Commands for tables

<code>delete</code> <code><table_name></code>	<p>Remove a table from the current object.</p> <p>For example, in <code>config system admin</code>, you could delete an administrator account named <code>newadmin</code> by typing <code>delete newadmin</code> and pressing Enter. This deletes <code>newadmin</code> and all its fields, such as <code>newadmin</code>'s name and email-address.</p> <p><code>delete</code> is only available within objects containing tables.</p>
<code>edit</code> <code><table_name></code>	<p>Create or edit a table in the current object.</p> <p>For example, in <code>config system admin</code>:</p> <ul style="list-style-type: none">• edit the settings for the default <code>admin</code> administrator account by typing <code>edit admin</code>.• add a new administrator account with the name <code>newadmin</code> and edit <code>newadmin</code>'s settings by typing <code>edit newadmin</code>. <p><code>edit</code> is an interactive sub-command: further sub-commands are available from within <code>edit</code>.</p> <p><code>edit</code> changes the prompt to reflect the table you are currently editing.</p> <p><code>edit</code> is only available within objects containing tables.</p>
<code>end</code>	<p>Save the changes to the current object and exit the <code>config</code> command. This returns you to the top-level command prompt.</p>

Table 2: Commands for tables

get	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values.
purge	<p>Remove all tables in the current object.</p> <p>For example, in <code>config forensic user</code>, you could type <code>get</code> to see the list of user names, then type <code>purge</code> and then <code>y</code> to confirm that you want to delete all users.</p> <p><code>purge</code> is only available for objects containing tables.</p> <p>Caution: Back up the FortiMail unit before performing a <code>purge</code>. <code>purge</code> cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see backup.</p> <p>Caution: Do not purge <code>system interface</code> or <code>system admin</code> tables. <code>purge</code> does not provide default tables. This can result in being unable to connect or log in, requiring the FortiMail unit to be formatted and restored.</p>
rename <table_name> to <table_name>	<p>Rename a table.</p> <p>For example, in <code>config system admin</code>, you could rename <code>admin3</code> to <code>fwadmin</code> by typing <code>rename admin3 to fwadmin</code>.</p> <p><code>rename</code> is only available within objects containing tables.</p>
show	<p>Display changes to the default configuration. Changes are listed in the form of configuration commands.</p>

Example of table commands

From within the `system admin` object, you might enter:

```
edit admin_1
```

The CLI acknowledges the new table, and changes the command prompt to show that you are now within the `admin_1` table:

```
new entry 'admin_1' added
(admin_1)#
```

Table 3: Commands for fields

abort	<p>Exit both the <code>edit</code> and/or <code>config</code> commands without saving the fields.</p>
end	<p>Save the changes made to the current table or object fields, and exit the <code>config</code> command. (To exit without saving, use <code>abort</code> instead.)</p>
get	<p>List the configuration of the current object or table.</p> <ul style="list-style-type: none"> • In objects, <code>get</code> lists the table names (if present), or fields and their values. • In a table, <code>get</code> lists the fields and their values.

Table 3: Commands for fields

next	<p>Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. (To save and exit completely to the root prompt, use <code>end</code> instead.)</p> <p><code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time.</p> <p><code>next</code> is only available from a table prompt; it is not available from an object prompt.</p>
set <field_name> <value>	<p>Set a field's value.</p> <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, you could type <code>set passwd newpass</code> to change the password of the <code>admin</code> administrator to <code>newpass</code>.</p> <p>Note: When using <code>set</code> to change a field containing a space-delimited list, type the whole new list. For example, <code>set <field> <new-value></code> will replace the list with the <code><new-value></code> rather than appending <code><new-value></code> to the list.</p>
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field_name>	<p>Reset the table or object's fields to default values.</p> <p>For example, in <code>config system admin</code>, after typing <code>edit admin</code>, typing <code>unset passwd</code> resets the password of the <code>admin</code> administrator account to the default (in this case, no password).</p>

Example of field commands

From within the `admin_1` table, you might enter:

```
set passwd my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the `passwd` field. You might then enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Depending on the account that you use to log in to the FortiMail unit, you may not have complete access to all CLI commands or areas of the web UI.

Access profiles and domain assignments together control which commands and areas an administrator account can access. **Permissions result from an interaction of the two.**

The domain to which an administrator is assigned can be either:

- **System:** Can access areas regardless of whether an item pertains to the FortiMail unit itself or to a protected domain. The administrator's permissions are restricted only by his or her access profile.
- a protected domain: Can **only** access areas that are specifically assigned to that protected domain. The administrator **cannot** access system-wide settings, files or statistics, nor most settings that can affect other protected domains, regardless of whether access to those items would otherwise be allowed by his or her access profile. The administrator **cannot**

access the CLI, nor the basic mode of the web UI. (For more information on the display modes of the GUI, see the [FortiMail Administration Guide](#).)



IP-based policies, the global black list, and the global white list, the blacklist action, and the global Bayesian database are exceptions to this rule. Domain administrators can configure them, regardless of the fact that they could affect other domains. If you do not want to allow this, do **not** provide *Read-Write* permission to those categories in domain administrators' access profiles.

Table 4: Areas of the GUI (advanced mode) that cannot be accessed by domain administrators

<i>Maintenance</i>
<i>Monitor except for the Personal quarantine tab</i>
<i>System except for the Administrator tab</i>
<i>Mail Settings except for the domain, its subdomains, and associated domains</i>
<i>User > User > PKI User</i>
<i>Policy > Access Control > Receive</i> <i>Policy > Access Control > Delivery</i>
<i>Profile > Authentication</i>
<i>AntiSpam except for AntiSpam > Bayesian > User and AntiSpam > Black/White List</i>
<i>Email Archiving</i>
<i>Log and Report</i>

Access profiles assign either read, write, or no access to each area of the FortiMail software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an access profile that administrator accounts can use, see [sensitive data](#).

Table 5: Areas of control in access profiles

Access control area name		Grants access to
In the web UI	In the CLI	<p>(For each <code>config</code> command, there is an equivalent <code>get/show</code> command, unless otherwise noted.</p> <p><code>config</code> access requires write permission. <code>get/show</code> access requires read permission.)</p>
Policy	policy	<p><i>Monitor > Mail Queue ...</i></p> <p><i>Monitor > Greylist ...</i></p> <p><i>Monitor > Sender Reputation > Display</i></p> <p><i>Mail Settings > Domains > Domains</i></p> <p><i>Mail Settings > Proxies > Proxies</i></p> <p><i>User > User ...</i></p> <p><i>Policy ...</i></p> <p><i>Profile ...</i></p> <p><i>AntiSpam > Greylist ...</i></p> <p><i>AntiSpam > Bounce Verification > Settings</i></p> <p><i>AntiSpam > Endpoint Reputation ...</i></p> <p><i>AntiSpam > Bayesian ...</i></p>
		<pre>config antispan greylist exempt config antispan bounce-verification key config antispan settings config domain config mailsetting proxy-smtp config policy ... config profile ... config user ...</pre>
Black/White List	black-white-list	<p><i>Monitor > Endpoint Reputation > Auto Blacklist</i></p> <p><i>Maintenance > AntiSpam > Black/White List Maintenance</i></p> <p><i>AntiSpam > Black/White List ...</i></p>
		N/A

Table 5: Areas of control in access profiles

Quarantine	quarantine	<p><i>Monitor > Quarantine ...</i></p> <p><i>AntiSpam > Quarantine > Quarantine Report</i></p> <p><i>AntiSpam > Quarantine > System Quarantine Setting</i></p> <p><i>AntiSpam > Quarantine > Control Account</i></p> <hr/> <p>config antispam quarantine-report</p> <p>config mailsetting systemquarantine</p>
Others	others	<p><i>Monitor > System Status ...</i></p> <p><i>Monitor > Archive > Email Archives</i></p> <p><i>Monitor > Log ...</i></p> <p><i>Monitor > Report ...</i></p> <p><i>Maintenance ... except the Black/White List Maintenance tab</i></p> <p><i>System ...</i></p> <p><i>Mail Settings > Settings ...</i></p> <p><i>Mail Settings > Address Book > Address Book</i></p> <p><i>User > User Alias > User Alias</i></p> <p><i>User > Address Map > Address Map</i></p> <p><i>Email Archiving ...</i></p> <p><i>Log and Report ...</i></p> <hr/> <p>config archive ...</p> <p>config log ...</p> <p>config mailsetting relayserver</p> <p>config mailsetting storage</p> <p>config report</p> <p>config system ...</p> <p>config user alias</p> <p>config user map</p> <p>diagnose ...</p> <p>execute ...</p> <p>get system status</p>

Unlike other administrator accounts whose *Access profile* is *super_admin_prof* and *Domain* is *System*, the `admin` administrator account exists by default and cannot be deleted. The `admin` administrator account is similar to a root administrator account. This administrator account always has full permission to view and change all FortiMail configuration options, including viewing and changing **all** other administrator accounts. It is the only administrator account that can reset another administrator's password without being required to enter the existing password. As such, it is the **only** account that can reset another administrator's password if that

administrator forgets his or her password. Its name, permissions, and assignment to the *System* domain cannot be changed.



Set a strong password for the `admin` administrator account, and change the password regularly. By default, this administrator account has no password. Failure to maintain the password of the `admin` administrator account could compromise the security of your FortiMail unit.

For complete access to all commands, you must log in with the administrator account named `admin`. For access to the CLI, you must log in with a *System*-level administrator account.

Tips and tricks

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

This section includes:

- [Help](#)
- [Shortcuts and key commands](#)
- [Command abbreviation](#)
- [Special characters](#)
- [Language support](#)
- [Baud rate](#)
- [Editing the configuration file on an external host](#)

Help

To display brief help during command entry, press the question mark (?) key.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Table 6: Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N

Table 6: Shortcuts and key commands

Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines.	Ctrl + C

Command abbreviation

In most cases, you can abbreviate words in the command line to their smallest number of non-ambiguous characters. For example, the command `get system status` could be abbreviated to `g sy st.`

Some commands may not be abbreviated. See the notes in the specific commands.

Special characters

The characters `<`, `>`, `(`, `)`, `#`, `'`, and `"` are not permitted in most CLI fields. These characters are special characters, sometimes also called reserved characters.

You may be able to enter a special character as part of a string's value by using a special command, enclosing it in quotes, or preceding it with an escape sequence — in this case, a backslash (`\`) character.

Table 7: Entering special characters

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (to be interpreted as part of a string value, not to end the string)	<p>Enclose the string in quotation marks: <code>"Security Administrator"</code>.</p> <p>Enclose the string in single quotes: <code>'Security Administrator'</code>.</p> <p>Precede the space with a backslash: <code>Security\ Administrator</code>.</p>
' (to be interpreted as part of a string value, not to end the string)	<code>\'</code>

Table 7: Entering special characters

" (to be interpreted as part of a string value, not to end the string)	\"
\	\\

Language support

Characters such as ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured.

For example, the host name must not contain special characters, and so the web UI and CLI will not accept most symbols and non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. But dictionary profiles support terms encoded in UTF-8, and therefore support a number of languages.

It is simplest to use only US-ASCII characters when configuring the FortiMail unit using the web UI or CLI. Using only ASCII, you do not need to worry about:

- mail transfer agent (MTA) encoding support
- mail user agent (MUA) language support
- web browser language support
- Telnet and/or SSH client support
- font availability
- compatibility of your input's encoding with the encoding/language setting of the web UI
- switching input methods when entering a command word such as `get` in ASCII but a setting that uses a different encoding



If you choose to configure parts of the FortiMail unit using non-ASCII characters, verify that all systems interacting with the FortiMail unit also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web UI and your web browser or Telnet/SSH client while you work.

Baud rate

You can change the default baud rate of the local console connection. For more information, see the *FortiMail Administration Guide*.

Editing the configuration file on an external host

You can edit the FortiMail configuration on an external host by first backing up the configuration file to a TFTP server. Then edit the configuration file and restore it to the FortiMail unit.

Editing the configuration on an external host can be time-saving if you have many changes to make, especially if your plain text editor provides advanced features such as batch changes.

To edit the configuration on your computer

1. Use `backup` to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style line endings.



Do not edit the first line. The first line(s) of the configuration file (preceded by a # character) contains information about the firmware version and FortiMail model. If you change the model number, the FortiMail unit will reject the configuration file when you attempt to restore it.

3. Use `restore config` to upload the modified configuration file back to the FortiMail unit.
The FortiMail unit downloads the configuration file and checks that the model information is correct. If it is, the FortiMail unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiMail unit ignores the command. If the configuration file is valid, the FortiMail unit restarts and loads the new configuration.

config

`config` commands configure your FortiMail settings.

This chapter describes the following commands:

antispam behavior-analysis	mailsetting storage central-ibe	system central-management
antispam bounce-verification key	mailsetting storage central-quarantine	system certificate local
antispam deepheader-analysis	mailsetting storage config	system certificate remote
antispam endpoint reputation blacklist	mailsetting systemquarantine	system ddns
antispam endpoint reputation exempt	policy access-control receive	system disclaimer
antispam greylist exempt	policy access-control delivery	system disclaimer-exclude
antispam quarantine-report	policy ip	system dns
antispam settings	policy recipient	system encryption ibe
antispam trusted	profile antispam	system encryption ibe-auth
archive account	profile antispam-action	system fortiguard antivirus
archive exempt-policy	profile antivirus	system fortiguard antispam
archive journal	profile antivirus-action	system fortisandbox
customized-message	profile authentication	system global
dlp scan-rules	profile certificate-binding	system ha
domain	profile content	system interface
domain-association	profile content-action	system mailserver
file filter	profile dictionary	system password-policy
file signature	profile dictionary-group	system port-forwarding
log setting remote	profile email-address-group	system route
log setting local	profile encryption	system saml
log alertemail recipient	profile ip-address-group	system scheduled-backup
log alertemail setting	profile ip-pool	system security authserver
mailsetting host-mapping	profile ldap	system snmp community
mailsetting mail-scan-options	profile notification	system snmp sysinfo
mailsetting preference	profile resource	system snmp threshold
mailsetting proxy-smtp	profile session	system snmp user
mailsetting relay-host-list	profile tls	system time manual
mailsetting sender-email-addr-handling	report	system time ntp
mailsetting smtp-rcpt-verification	sensitive data	system webmail-language
	system admin	system wccp settings
	system appearance	user alias
	system backup-restore-mail	user map
		user pki

antispam behavior-analysis

Use this command to analyze the similarity of uncertain email against those well-known spam messages which are received recently.

Syntax

```
config antispam behavior-analysis
  set status {enable | disable}
  set analysis-level {high | medium | low}
end
```

Variable	Description	Default
status {enable disable}	Enable or disable behavior analysis service.	enable
analysis-level {high medium low}	Enter the analysis level.	medium

Related topics

- [antispam deepheader-analysis](#)
- [antispam greylist exempt](#)
- [antispam quarantine-report](#)
- [antispam settings](#)
- [antispam trusted](#)

antispam bounce-verification key

Use this command to configure bounce address tagging and verification (BATV) keys.

Syntax

```
config antispam bounce-verification key
  edit <key_str>
    set status {active | inactive}
  next
end
```

Variable	Description	Default
<key_str>	Enter a new or existing key.	No default.
status {active inactive}	Enable or disable usage of the key.	inactive

Related topics

- [antispam deepheader-analysis](#)
- [antispam greylist exempt](#)
- [antispam quarantine-report](#)
- [antispam settings](#)
- [antispam trusted](#)

antispam deepheader-analysis

Use this command to configure global deepheader-analysis scan settings used by antispam profiles.

Deepheader analysis examines the entire message header for spam characteristics.

Not all headers may be checked, depending on your configuration of “antispam trusted” on [page 44](#).

Syntax

```
config antispam deepheader-analysis
    set confidence <percent_float>
    set greyscale-level <level_int>
end
```

Variable	Description	Default
confidence <percent_float>	Type the confidence percentage above which a message will be considered spam. The deep header scan examines each message and calculate a confidence value based on the results of the decision-tree analysis. The higher the calculated confidence value, the more likely the message is really spam. The deep header scan adds an X-FEAS-DEEPHEADER: line to the message header that includes the message's calculated confidence value.	95.00000 0
greyscale-level <level_int>	Type the grey scale threshold above which the deepheader scan will be skipped. FortiGuard antispam service uses the grey scale of 1-9 to determine spam. 1-4 means the email is a spam for sure, while 9 is not a spam for sure. Therefore, increasing this grey scale level will increase the probability to scan the email. This may increase spam catch rate but also increase false positives.	7

Related topics

- [profile antispam](#)
- [antispam trusted](#)
- [antispam greylist exempt](#)
- [antispam settings](#)

antispam endpoint reputation blacklist

Use this command to manually blacklist carrier end points by MSISDN.

MSISDN numbers listed on the black list will have their email or text messages blocked as long as their identifier appears on the black list.

Syntax

```
config antispam endpoint reputation blacklist
    edit <msisdn>
end
```

Variable	Description	Default
<msisdn>	Type the MSISDN number to blacklist carrier end point.	

Related topics

- [profile antispam](#)
- [antispam trusted](#)

antispam endpoint reputation exempt

Use this command to manually exempt carrier end points by MSISDN from automatic blacklisting due to their endpoint reputation score.

Syntax

```
config antispam endpoint reputation exempt
    edit <msisdn>
end
```

Variable	Description	Default
<msisdn>	Type the MSISDN number to exempt carrier end point.	

Related topics

- [antispam endpoint reputation blacklist](#)

antispam greylist exempt

Use this command to configure the greylist exempt list.

Greylist scanning blocks spam based on the behavior of the sending server, rather than the content of the messages. When receiving an email from an unknown server, the FortiMail unit will temporarily reject the message. If the mail is legitimate, the originating server will try to send it again later ([RFC 2821](#)), at which time the FortiMail unit will accept it. Spam senders rarely attempt a retry.

Syntax

```

config antisppam greylist exempt
  edit <entry_index>
    set recipient-pattern <recipient_pattern>
    set recipient-pattern-regexp {enable | disable}
    set reverse-dns-pattern <reverse-dns_pattern>
    set reverse-dns-pattern-regexp {enable | disable}
    set sender-ip <client_ipv4/mask>
    set sender-pattern <sender_pattern>
    set sender-pattern-regexp {enable | disable}
  next
end

```

Variable	Description	Default
<entry_index>	Greylist exempt rule ID.	No default.
recipient-pattern <recipient_pattern>	Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as \'*\').	No default.
recipient-pattern-regexp {enable disable}	<ul style="list-style-type: none"> Enter enable if you used regular expression syntax to define the pattern. Enter disable if you did not use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?). 	disable
reverse-dns-pattern <reverse-dns_pattern>	Enter a pattern that defines reverse DNS query responses which match this rule, surrounded in slashes and single quotes (such as \'*\').	No default.
reverse-dns-pattern-regexp {enable disable}	<ul style="list-style-type: none"> Enter enable if you used regular expression syntax to define the pattern. Enter disable if you did not use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?). 	disable
sender-ip <client_ipv4/mask>	Enter the IP address and netmask of the SMTP client. To match SMTP sessions from any SMTP client, enter 0.0.0.0/0.	No default.
sender-pattern <sender_pattern>	Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as \'*@example.com\').	No default.
sender-pattern-regexp {enable disable}	<ul style="list-style-type: none"> Enter enable if you used regular expression syntax to define the pattern. Enter disable if you did not use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?). 	disable

Related topics

- [antispam bounce-verification key](#)
- [antispam deepheader-analysis](#)
- [antispam quarantine-report](#)
- [antispam settings](#)
- [antispam trusted](#)

antispam quarantine-report

Use these commands to configure global settings for quarantine reports.

Quarantine reports notify email users of email added to their per-recipient quarantine, and allow them to release or delete email from the quarantine.

Alternatively, you can configure quarantine report settings specifically for each protected domain. For details, see [“config domain-setting” on page 81](#).

Syntax

```
config antispam quarantine-report
  set report-template-name {default | default-with-icons}
  set schedule-days <days_str>
  set schedule-hours <hour_int>
  set web-release-hostname <FortiMail_fqdn>
  set web-release-https {enable | disable}
  set web-release-unauth-expiry <hour_int>
end
```

Variable	Description	Default
report-template-name {default default-with-icons}	Enter a report template.	default
schedule-days <days_str>	Enter a comma-delimited list of days off the week on which the FortiMail unit will generate spam reports.	No default.
schedule-hours <hour_int>	Enter a comma-delimited list of numbers corresponding to the hours of the day on which the FortiMail unit will generate spam reports. For example, to generate spam reports on 1:00 AM, 2:00 PM, and 11:00 PM, you would enter 1, 14, 23. Valid numbers are from 0 to 23, based upon a 24-hour clock.	No default.
web-release-hostname <FortiMail_fqdn>	Enter an alternate resolvable fully qualified domain name (FQDN) to use in web release hyperlinks that appear in spam reports.	No default.

Variable	Description	Default
web-release-https {enable disable}	Enable to redirect HTTP requests for FortiMail webmail and per-recipient quarantines to secure access using HTTPS. Note: For this option to function properly, you must also enable both HTTP and HTTPS access protocols on the network interface to which the email user is connecting.	enable
web-release-unauth-expiry <hour_int>	Enter the period of time after the spam report is generated during which the email user can access the per-recipient quarantine without authenticating. To require the user enter a user name and password, enter 0. Valid values are from 0 to 720. Note: If you require email users to authenticate, in order to define their user name and password, you must configure either local user accounts, or authentication profiles applied through an inbound recipient-based policy.	0

Related topics

- [antispam bounce-verification key](#)
- [antispam deepheader-analysis](#)
- [antispam greylist exempt](#)
- [antispam settings](#)
- [antispam trusted](#)

antispam settings

Use these commands to configure global antispam settings.

Syntax

```
config antispam settings
  set backend_verify <time_str>
  set bayesian-is-not-spam <local-part_str>
  set bayesian-is-spam <local-part_str>
  set bayesian-learn-is-not-spam <local-part_str>
  set bayesian-learn-is-spam <local-part_str>
  set bayesian-training-group <local-part_str>
  set blacklist-action {as-profile | discard | reject}
  set bounce-verification-action {as-profile | discard | reject}
  set bounce-verification-auto-delete-policy {never | one-month |
    one-year | six-months | three-months}
  set bounce-verification-status {enable | disable}
  set bounce-verification-tagexpiry <days_int>
  set carrier-endpoint-acct-response {enable | disable}
  set carrier-endpoint-acct-secret <password_str>
  set carrier-endpoint-acct-validate {enable | disable}
  set carrier-endpoint-attribute {Acct-Authentic ...
    Vendor-Specific}
  set carrier-endpoint-blacklist-window-size {quarter | half-hour |
    one-hour | two-hours | four-hours | six-hours | eight-hours |
    one-day}
  set carrier-endpoint-framed-ip-attr {Framed-IP- Address |
    Login-IP-Host | Login-IPv6-Host | NAS-IP-Address |
    NAS-IPv6-Address}
  set carrier-endpoint-framed-ip-order {host-order | network-order}
  set carrier-endpoint-radius-port <port_int>
  set carrier-endpoint-status {enable | disable}
  set delete-ctrl-account <local_part_str>
  set greylist-capacity <maximum_int>
  set greylist-delay <1-120 minutes>
  set greylist-init-expiry-period <window_int>
  set greylist-ttl <tll_int>
  set release-ctrl-account <local-part_str>
  set safe-block-list-precedence {system session domain personal}
  set session-profile-rate-control-interval <minutes>
  set spf-checking {aggressive | aggressive-anti-spoofing | strict |
    strict-anti-spoofing}
  set uri-checking {aggressive | strict}
end
```

Variable	Description	Default
backend_verify <time_str>	<p>Enter the time of day at which the FortiMail unit will automatically remove invalid per-recipient quarantines. Use the format <code>hh:mm:ss</code>, where <code>hh</code> is the hour according to a 24-hour clock, <code>mm</code> is the minute, and <code>ss</code> is the second.</p> <p>For example, to begin automatic invalid quarantine removal at 5:30 PM, enter <code>17:30:00</code>.</p>	4:0:0
bayesian-is-not-spam <local-part_str>	<p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that correct false positives.</p> <p>For example, if the local domain name of the FortiMail unit is <code>example.com</code> and you want to correct the assessment of a previously scanned spam that was actually legitimate email by sending control messages to <code>is-not-spam@example.com</code>, you would enter <code>is-not-spam</code>.</p>	is-not-spam
bayesian-is-spam <local-part_str>	<p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that correct false negatives.</p> <p>For example, if the local domain name of the FortiMail unit is <code>example.com</code> and you want to correct the assessment of a previously scanned email that was actually spam by sending control messages to <code>is-spam@example.com</code>, you would enter <code>is-spam</code>.</p>	is-spam
bayesian-learn-is-not-spam <local-part_str>	<p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that train it to recognize legitimate email.</p> <p>Unlike the <code>is-not-spam</code> email address, this email address will receive email that has not been previously seen by the Bayesian scanner.</p> <p>For example, if the local domain name of the FortiMail unit is <code>example.com</code> and you want to train the Bayesian database to recognize legitimate email by sending control messages to <code>learn-is-not-spam@example.com</code>, you would enter <code>learn-is-not-spam</code>.</p>	learn-is-not-spam
bayesian-learn-is-spam <local-part_str>	<p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that train it to recognize spam.</p> <p>Unlike the <code>is-spam</code> email address, this email address will receive spam that has not been previously seen by the Bayesian scanner.</p> <p>For example, if the local domain name of the FortiMail unit is <code>example.com</code> and you want to train the Bayesian database to recognize spam by sending control messages to <code>learn-is-spam@example.com</code>, you would enter <code>learn-is-spam</code>.</p>	learn-is-spam

Variable	Description	Default
bayesian-training-group <code><local-part_str></code>	<p>Enter the local-part portion of the email address that FortiMail administrators can use as their sender email address when forwarding email to the “learn is spam” email address or “learn is not spam” email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain) but will not train any per-user Bayesian database.</p> <p>In contrast, if a FortiMail administrator were to forward email using their own email address (rather than the training group email address) as the sender email address, and per-user Bayesian databases were enabled in the corresponding incoming antispam profile, the FortiMail unit would also apply the training message to their own per-user Bayesian database.</p>	default-group
blacklist-action <code>{as-profile discard reject}</code>	<p>Use these commands to select the action that the FortiMail unit performs when an email message arrives from or, in the case of per-session profile recipient black lists, is destined for a blacklisted email address, mail domain, or IP address.</p> <p>This setting affects email matching any system-wide, per-domain, per-session profile, or per-user blacklist.</p> <p>For email messages involving a blacklisted email address, domain, or IP address, select one of the following options:</p> <ul style="list-style-type: none"> as-profile: Apply the action selected in the antispam profile being applied to the email message. For details, see “profile antispam-action” on page 172. discard: Accept the message but delete and do not deliver it, without notifying the SMTP client. reject: Reject the message, returning an SMTP error code to the SMTP client. 	reject
bounce-verification-action <code>{as-profile discard reject}</code>	<p>Enter the action that the FortiMail unit will perform if it receives a bounce address tag that is invalid.</p> <ul style="list-style-type: none"> as-profile: Perform the action selected in the antispam profile. discard: Accept the message but then delete it without notifying the SMTP client. reject: Reject the message, replying to the SMTP client with an SMTP rejection code. 	as-profile

Variable	Description	Default
<pre>bounce-verification-auto-delete-policy {never one-month one-year six-months three-months}</pre>	<p>Inactive keys will be removed after being unused for the selected time period.</p> <ul style="list-style-type: none"> never: Never automatically delete an unused key. one-month: Delete a key when it hasn't been used for 1 month. three-months: Delete a key when it hasn't been used for 3 months. six-months: Delete a key when it hasn't been used for 6 months. one-year: Delete a key when it hasn't been used for 12 months. <p>The active key will not be automatically removed.</p>	never
<pre>bounce-verification-status {enable disable }</pre>	<p>Enable to activate bounce address tagging and verification.</p> <p>Tag verification can be bypassed in IP profiles and protected domains.</p>	disable
<pre>bounce-verification-tagexpiry <days_int></pre>	<p>Enter the number of days an email tag is valid. When this time elapses, the FortiMail unit will treat the tag as invalid.</p> <p>Valid range is from 3 to 30 days.</p>	7
<pre>carrier-endpoint-acct-response {enable disable }</pre>	<p>Enable/disable endpoint account validation on the RADIUS server.</p>	disable
<pre>carrier-endpoint-acct-secret <password_str></pre>	<p>Type the shared secret for RADIUS account response/request validation.</p>	
<pre>carrier-endpoint-acct-validate {enable disable }</pre>	<p>Enable/disable validating shared secret of account requests.</p>	disable

Variable	Description	Default
carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific)	<p>Type the RADIUS account attribute associated with the endpoint user ID. If you have more than one RADIUS server and each server uses different account attribute for the endpoint user ID, you can specify up to five attributes with this command. For example, a 3G network may use the “Calling-Station-ID” attribute while an ADSL network may use the “User-Name” attribute.</p> <p>A carrier end point is any device on the periphery of a carrier’s or Internet service provider’s (ISP) network. It could be a subscriber’s GSM cellular phone, wireless PDA, or computer using DSL service.</p> <p>Unlike MTAs, computers in homes and small offices and mobile devices such as laptops and cellular phones that send email may not have a static IP address. Cellular phones’ IP addresses especially may change very frequently. After a device leaves the network or changes its IP address, its dynamic IP address may be reused by another device. Because of this, a sender reputation score that is directly associated with an SMTP client’s IP address may not function well. A device sending spam could start again with a clean sender reputation score simply by rejoining the network to get another IP address, and an innocent device could be accidentally blacklisted when it receives an IP address that was previously used by a spammer.</p>	Calling-Station-Id (RADIUS attribute 31)
carrier-endpoint-blacklist-window-size {quarter half-hour one-hour two-hours four-hours six-hours eight-hours one-day}	<p>Enter the amount of previous time, in minutes, whose score-increasing events will be used to calculate the current endpoint reputation score.</p> <p>For example, if the window is a quarter (15 minutes), detections of spam or viruses 0-15 minutes ago would count towards the current score; detections of spam or viruses older than 15 minutes ago would not count towards the current score.</p>	quarter
carrier-endpoint-framed-ip-attr {Framed-IP-Address Login-IP-Host Login-IPv6-Host NAS-IP-Address NAS-IPv6-Address}	<p>Specify the RADIUS attribute whose value will be used as the endpoint user IP address.</p> <p>By default, the endpoint user IP address uses the value of RADIUS attribute 8 (framed IP address).</p> <p>However, if the endpoint IP address uses the value from different RADIUS attribute/number other than attribute 8, you can specify the corresponding attribute number with this command.</p> <p>You can use the “diagnose debug application msisdn” command to capture RADIUS packets and find out what attribute name/number is used to hold the IP address value.</p> <p>Note that you can specify multiple values, such as both IPv4 and IPv6 attributes.</p>	Framed-IP-Address

Variable	Description	Default
carrier-endpoint-framed-ip-order {host-order network-order}	<p>Select one of the following methods for endpoint IP address formatting:</p> <ul style="list-style-type: none"> host-order: format an IP address in host order, that is, the host portion is at the beginning. For example, 1.1.168.192. network-order: sorts IP addresses in the network order, that is, the network portion is at the beginning. For example, 192.168.1.1. 	host-order
carrier-endpoint-radius-port <port_int>	Type the RADIUS server port for carrier endpoint account requests.	1813
carrier-endpoint-status {enable disable }	<p>Enable endpoint reputation scan for traffic examined by the session profile.</p> <p>This command starts the endpoint reputation daemon. You must start this daemon for the endpoint reputation feature to work.</p>	enable
delete-ctrl-account <local_part_str>	<p>Use this command to configure the email addresses through which email users can delete email from their per-recipient quarantines.</p> <p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines.</p> <p>For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter quar_delete.</p>	delete-ctrl
greylist-capacity <maximum_int>	<p>Enter the maximum number of greylist items in the greylist. New items that would otherwise cause the greylist database to grow larger than the capacity will instead overwrite the oldest item.</p> <p>To determine the default value and acceptable range for your FortiMail model, enter a question mark (?).</p>	Varies by model

Variable	Description	Default
greylist-delay <1-120 minutes>	<p>Enter the length in minutes of the greylist delay period.</p> <p>For the initial delivery attempt, if no manual greylist entry (exemption) matches the email message, the FortiMail unit creates a pending automatic greylist entry, and replies with a temporary failure code. During the greylist delay period after this initial delivery attempt, the FortiMail unit continues to reply to additional delivery attempts with a temporary failure code.</p> <p>After the greylist delay period elapses and before the pending entry expires (during the <code>initial_expiry_period</code>, also known as the greylist window), any additional delivery attempts will confirm the entry and convert it to an individual automatic greylist entry. The greylist scanner will then allow delivery of subsequent matching email messages.</p> <p>The valid range between 1 and 120 minutes.</p>	10
greylist-init-expiry-period <window_int>	<p>Enter the period of time in hours after the <code>greylistperiod</code>, during which pending greylist entries will be confirmed and converted into automatic greylist entries if the SMTP client retries delivery.</p> <p>The valid range is from 4 to 24 hours.</p>	4
greylist-ttl <ttl_int>	<p>Enter the time to live (TTL) that determines the maximum amount of time that unused automatic greylist entries will be retained.</p> <p>Expiration dates of automatic greylist entries are determined by adding the TTL to the date and time of the previous matching delivery attempt. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire.</p> <p>If the TTL elapses without an email message matching the automatic greylist entry, the entry expires and the greylist scanner removes the entry.</p> <p>The valid range is between 1 and 60 days.</p>	30

Variable	Description	Default
release-ctrl-account <local-part_str>	<p>Use this command to configure the email addresses through which email users can release email from their per-recipient quarantines.</p> <p>Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines.</p> <p>For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter quar_delete.</p>	No default.
safe-block-list-precedence {system session domain personal}	By default, system safelists and blocklists have precedence over other safelists and blocklists. In some cases, you may want to change the precedence order. For example, you may want to allow a user to use his/her own lists to overwrite the system list. In this case, you can move "personal" ahead of "system".	system session domain personal
session-profile-rate-control-interval <minutes>	<p>The rate control option enables you to control the rate at which email messages can be sent, by the number of connections, the number of messages, or the number recipients per client per period (in minutes).</p> <p>This command sets the time period. Other values are set under the <code>config profile session</code> command.</p>	30

Variable	Description	Default
spf-checking {aggressive aggressive-anti-spoofing strict strict-anti-spoofing}	<p>Sender Policy Framework (SPF) DNS records allow domain owners to publish the IP addresses authorized to send email on their behalf. FortiMail will check the SMTP client IP address against the published IP addresses in the DNS records. This is to prevent malicious spam senders to disguise their identities.</p> <p>When you configure a session profile or an antispam profile, you can enable/disable SPF checking.</p> <p>Before FortiMail 4.0 MR3 Patch 1 release, only SPF hardfailed (-all) email is treated as spam. Starting from 4.0 MR3 Patch 2 release, you can use this CLI command to control if the SPF softfailed (~all) email should also be treated as spam.</p> <ul style="list-style-type: none"> aggressive: Choose this option to treat both the SPF hardfailed and softfailed email as spam. This option checks the envelope MAIL FROM address only. aggressive-anti-spoofing: Choose this option to treat both the SPF hardfailed and softfailed email as spam. This option checks both the envelope MAIL FROM and header From addresses to detect spoofing. strict: Choose this option to treat only the SPF hardfailed email as spam. This option checks the envelope MAIL FROM address only. strict-anti-spoofing: Choose this option to treat only the SPF hardfailed email as spam. This option checks both the envelope MAIL FROM and header From addresses to detect spoofing. 	strict

Variable	Description	Default
uri-checking {aggressive strict}	<p>When you configure an antispam profile under <i>Profile</i> > <i>AntiSpam</i> > <i>AntiSpam</i>, if you enable FortiGuard scan and SURBL scan, FortiMail will scan for blacklisted URIs in email bodies.</p> <p>There are two types of URIs:</p> <ul style="list-style-type: none"> Absolute URIs strictly follow the URI syntax and include the URI scheme names, such as “http”, “https”, and “ftp”. For instance, http://www.example.com. Reference URIs do not contain the scheme names. For instance, example.com. <p>In some cases, you may want to scans for both absolute and reference URIs to improve the catch rate.</p> <p>In some cases (for example, to lower false positive rates), you may want to scan for absolute URIs only.</p> <ul style="list-style-type: none"> aggressive: Choose this option to scan for both the absolute and reference URIs. strict: Choose this option to scan for absolute URIs only. Note that web sites without “http” or “https” but starting with “www” are also treated as absolute URIs. For instance, www.example.com. 	<p>aggressive (before v4.3.1 release)</p> <p>strict (after 4.3.2 release)</p>

Related topics

- [antispam bounce-verification key](#)
- [antispam deepheader-analysis](#)
- [antispam greylist exempt](#)
- [antispam quarantine-report](#)
- [antispam trusted](#)

antispam trusted

Use these commands to configure both the IP addresses of mail transfer agents (MTAs) that are trusted to insert genuine `Received:` message headers, and the IP addresses of MTAs that perform antispam scans before the FortiMail unit.

`Received:` message headers are inserted by each mail transfer agent (MTA) that handles an email message in route to its destination. The IP addresses in those headers can be used as part of FortiGuard Antispam and DNSBL antispam checks, and SPF and DKIM sender validation. However, they should only be used if you trust that the `Received:` header added by an MTA is not fake — spam-producing MTAs sometimes insert fake headers containing the IP addresses of legitimate MTAs in an attempt to circumvent antispam measures.

If you trust that `Received:` headers containing specific IP addresses are always genuine, you can add those IP addresses to the `mta` list.

Note that private network addresses, defined in RFC 1918, are never checked and do not need to be excluded using `config antispam trusted mta`.

Relatedly, if you can trust that a previous mail hop has already scanned the email for spam, you can add its IP address to the `antispam-mta` list to omit deep header scans for email that has already been evaluated by that MTA, thereby improving performance.

Syntax

```
config antispam trusted {mta | antispam-mta}
    edit <smtp_ipv4/mask>
end
```

Variable	Description	Default
<smtp_ipv4/mask>	Enter the IP address and netmask of an MTA.	No default.

Related topics

- [antispam bounce-verification key](#)
- [antispam deepheader-analysis](#)
- [antispam greylist exempt](#)
- [antispam quarantine-report](#)
- [antispam settings](#)

archive account

Use this command to configure email archiving accounts.

This command applies only if email archiving is enabled.

Syntax

```
config archive account
```

```

edit <account_name>
    set destination {local | remote}
    set forward-address <recipient_email>
    set imap-access {enable | disable}
    set index-type {full | header | none}
    set local-quota <quota_int>
    set local-quota-cache <cache_int>
    set password <password>
    set quota-full {overwrite | noarchive}
    set remote-directory <path_str>
    set remote-ip <ftp_ipv4>
    set remote-password <password_Str>
    set remote-protocol {ftp | sftp}
    set remote-username <user_str>
    set retention-period <year_int>
    set rotation-hour <hour_int>
    set rotation-size <size_int>
    set rotation-time <time_int>
    set status {enable | disable}
end

```

Variable	Description	Default
<account_name>	Enter the email archiving account name.	archive
destination {local remote}	Select whether to archive to the local disk or remote server.	local
forward-address <recipient_email>	Enter the email address to which all archived messages will also be forwarded. If no forwarding address exists, the FortiMail unit will not forward email when it archives it.	No default.
imap-access {enable disable}	Enable/disable IMAP access to the archive account.	No default.
index-type {full header none}	Type full to index email by the whole email (header and body), and header by the email header only.	none
local-quota <quota_int>	Enter the local disk quota for email archiving in gigabytes (GB). The valid range depends on the amount of free disk space.	5
local-quota-cache <cache_int>	Enter the local disk quota for caching in gigabytes (GB). The valid range depends on the amount of free disk space.	5
password <password>	Enter the password for the account access.	forti12356 net

Variable	Description	Default
quota-full {overwrite noarchive}	Enter either: <ul style="list-style-type: none"> noarchive: Discard the email message if the hard disk space is consumed and a new email message arrives. overwrite: Replace the oldest email message if the hard disk space is consumed and a new email message arrives. 	overwrite
remote-directory <path_str>	Enter the directory path on the remote server where email archives will be stored.	No default.
remote-ip <ftp_ipv4>	Enter the IP address of the remote server that will store email archives.	0.0.0.0
remote-password <password_Str>	Enter the password of the user account on the remote server.	No default.
remote-protocol {ftp sftp}	Enter either ftp or sftp to use that protocol when transferring email archives to the remote server.	sftp
remote-username <user_str>	Enter the name of a user account on the remote server.	No default.
retention-period <year_int>	Enter the time to keep archived messages in years (0 to keep forever).	0
rotation-hour <hour_int>	Enter the hour of the day to start the mailbox rotation. See rotation-time <time_int> .	0
rotation-size <size_int>	Enter the maximum size of the current email archiving mailbox in megabytes (MB). When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 10 to 200 MB.	100
rotation-time <time_int>	Enter the maximum age of the current email archiving mailbox in days. When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 1 to 365 days. See rotation-hour <hour_int>	7
status {enable disable }	Enable to activate email archiving.	disable

Related topics

- [archive exempt-policy](#)
- [archive journal](#)

archive exempt-policy

Use this command to configure the exemptions to email archiving.

This command applies only if email archiving is enabled.

Syntax

```
config archive exempt-policy
  edit <policy_id>
    set account <account_name>
    set pattern <string>
    set status {enable | disable}
    set type {attachment | body | recipient | sender | subject}
  end
```

Variable	Description	Default
<policy_id>	Enter the index number of the exemption policy. To view a list of existing entries, enter a question mark (?).	No default.
account <account_name>	Enter the name of the email archive account that you want to apply the exemption policy to.	
pattern <string>	Enter a pattern, such as <code>user*@example.com</code> , that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this exemption will apply.	*
status {enable disable }	Enable to activate the email archiving exemption.	enable
type {attachment body recipient sender subject}	Enter one of the following exemption match types: <ul style="list-style-type: none">• attachment: The attachment file name will be evaluated for matches with <code>pattern</code>.• body: The body text will be evaluated for matches with <code>pattern</code>.• recipient: The recipient email address will be evaluated for matches with <code>pattern</code>.• sender: The sender email address will be evaluated for matches with <code>pattern</code>.• subject: The email subject will be evaluated for matches with <code>pattern</code>.	

Related topics

- [archive journal](#)
- [archive account](#)

archive journal

Microsoft Exchange servers can journal email and then send the journaled email to another server, such as FortiMail, for archiving.

Syntax

```
config archive journal source
  edit <journal_source_id>
    set comments
    set host
    set recipient
    set sender
  end
```

Variable	Description	Default
<journal_source_id>	Enter the ID of the journal.	
comments	Enter general journal source comments.	
host	Enter the ip address or host name of the journal source.	
recipient	Enter the recipient email address.	
sender	Enter the sender email address.	

archive policy

Use this command to configure email archiving policies.

This command applies only if email archiving is enabled.

Syntax

```
config archive policy
  edit <policy_id>
    set account <account_name>
    set pattern <string>
    set status {enable | disable}
    set type {attachment | body | recipient | sender | subject}
  end
```

Variable	Description	Default
<policy_id>	Enter the index number of the policy. To view a list of existing entries, enter a question mark (?).	No default.
account <account_name>	Enter the name of the email archive account where you want to archive email.	
pattern <string>	Enter a pattern, such as <code>user*@example.com</code> , that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this policy will apply.	*

Variable	Description	Default
status {enable disable }	Enable to activate the email archiving policy.	enable
type {attachment body recipient sender subject}	Enter one of the following match types: <ul style="list-style-type: none"> • attachment: The attachment file name will be evaluated for matches with <code>pattern</code>. • body: The body text will be evaluated for matches with <code>pattern</code>. • recipient: The recipient email address will be evaluated for matches with <code>pattern</code>. • sender: The sender email address will be evaluated for matches with <code>pattern</code>. • subject: The email subject will be evaluated for matches with <code>pattern</code>. 	

Related topics

- [archive exempt-policy](#)
- [archive account](#)

customized-message

Use this command to configure replacement messages.

When the FortiMail unit detects a virus in an email attachment, it replaces the attachment with a message that provides information about the virus and source of the email.

The FortiMail unit may also use replacement messages when notifying a recipient that it has blocked an email as spam or due to content filtering, or when sending a quarantine report.

You can customize the secure message notifications that secure email recipients receive when IBE encrypted email are sent to them. configure simple network management protocol (SNMP) settings.

Syntax

This command contains many sub-commands. Each sub-command, linked in the table below, is documented in subsequent sections.

```
config customized-message
  edit <message_name>
  next
end
```

Variable	Description	Default
<message_name>	<p>Select the replacement message that you want to customize.</p> <p>The message name include:</p> <ul style="list-style-type: none"> • alert-email • as-sender-rate-notify • calendar-event-notify • custom-webmail-login • email-template-av-repack • email-template-notify-generic • ibe-banner-footer • ibe-banner-header • ibe-notify-account-reset • ibe-notify-account-reset-done • ibe-notify-password-reset • ibe-notify-password-reset-done • ibe-notify-pull-message • ibe-notify-push-message • ibe-notify-user-register-done • ibe-notify-wread-notif • ibe-notify-wunread-rcpt • ibe-notify-wunread-sender • log-report • login-disclaimer • reject-content-attachment • reject-content-message • reject-delivery • reject-endpoint-reputation • reject-spam • reject-virus-message • reject-virus-suspicious • replace-content-attachment • replace-content-body • replace-content-subject • replace-virus-message • replace-virus-suspicious • report-quarantine-summary 	No default.

Related topics

- [config domain-setting](#)
- [config policy recipient](#)

alert-email

Use this sub-command to configure the variables and the default email template of the alert email.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit alert-email
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%MEETING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%MEETING%% can be weekly meeting.	
from <string>	Enter the replacement message for the <code>from</code> field of the event notification email.	
html-body <string>	Enter the replacement message for the email body in HTML code.	
subject <string>	Enter the replacement message for the <code>subject</code> field of the notification.	
text-body <string>	Enter the replacement message for the email body in text format.	

as-sender-rate-notify

Use this sub-command to configure the variables and the default email template of the notifications for spam sender's sending rate.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit as-sender-rate-notify
  config variable
    edit <name>
      set content
      set display-name
  config email-template
    edit default
      set env-from <string>
      set from <string>
      set html-body <string>
      set subject <string>
      set text-body <string>
      set to <string>
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%MEETING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%MEETING%% can be weekly meeting.	
env-from <string>	Enter the replacement message for the email Envelope From field.	
from <string>	Enter the replacement message for the email From field.	
html-body <string>	Enter the replacement email body in HTML format.	
subject <string>	Enter the replacement message for the email Subject header.	
text-body <string>	Enter the replacement email body in text format.	
to <string>	Enter the replacement message for the email To field.	

calendar-event-notify

Use this sub-command to configure the variables and the default email template of the notification for calendar events in FortiMail webmail.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit calendar-event-notify
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%MEETING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%MEETING%% can be weekly meeting.	
from <string>	Enter the replacement message for the <code>from</code> field of the event notification email.	
html-body <string>	Enter the replacement message for the email body in HTML code.	
subject <string>	Enter the replacement message for the <code>subject</code> field of the notification.	
text-body <string>	Enter the replacement message for the email body in text format.	

custom-webmail-login

Use this sub-command to configure the variables and the default content of the webmail login.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit custom-webmail-login
  config variable
    edit <name>
      set content
      set display-name
    config message
      edit default
        set content <string>
        set format {html | multiline | text}
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%FILE%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%FILE%% can be Login.	
content <string>	Enter the replacement message for the webmail login.	
format {html multiline text}	Select the format for the webmail login.	html

email-template-av-repack

Use this sub-command to configure the variables and the default content of the email template for antivirus action.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit email-template-av-repack
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%FILE%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%FILE%% can be Template.	
from <string>	Enter the replacement message for the email From field.	
html-body <string>	Enter the replacement email body in HTML format.	
subject <string>	Enter the replacement message for the email Subject field.	
text-body <string>	Enter the replacement email body in text format.	

email-template-notify-generic

Use this sub-command to configure the variables and the default content of the email template for generic notifications.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit email-template-notify-generic
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set env-from <string>
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
        set to <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%FILE%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%FILE%% can be Template.	
env-from <string>	Enter the replacement message for the email Envelope From field.	
from <string>	Enter the replacement message for the email From field.	
html-body <string>	Enter the replacement email body in HTML format.	
subject <string>	Enter the replacement message for the email Subject header.	
text-body <string>	Enter the replacement email body in text format.	
to <string>	Enter the replacement message for the email To field.	

ibe-banner-footer

Use this sub-command to configure the variables and the default content of the secure message footer.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-banner-footer
  config variable
    edit <name>
      set content
      set display-name
    config message
      edit default
        set content <string>
        set format {html | multiline | text}
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SERVICE_NAME%%.	
content	Enter the content for the variable. For example, you may enter copyright information of the secure message.	
display-name	Enter the display name for the variable. For example, the display name for %%SERVICE_NAME%% can be Copyright.	
content <string>	Enter the replacement message for the secure message footer.	
format {html multiline text}	Select the format for the secure message footer.	html

ibe-banner-header

Use this sub-command to configure the variables and the default content of the secure message header.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-banner-header
  config variable
    edit <name>
      set content
      set display-name
    config message
      edit default
        set content <string>
        set format {html | multiline | text}
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SERVICE_NAME%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SERVICE_NAME%% can be Email header.	
content <string>	Enter the replacement message for the secure message header.	
format {html multiline text}	Select the format for the secure message header.	html

ibe-notify-account-reset

Use this sub-command to configure the variables and the default email template of the IBE account reset notification.

Syntax

This sub-command is available from within the command `customized-message`.

```

edit ibe-notify-account-reset
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end

```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-account-reset-done

Use this sub-command to configure the variables and the default email template of the IBE account reset completion notification.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-account-reset-done
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-password-reset

Use this sub-command to configure the variables and the default email template of the IBE password reset notification.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-password-reset
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-password-reset-done

Use this sub-command to configure the variables and the default email template of the IBE password reset completion notification.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-password-reset-done
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-pull-message

Use this sub-command to configure the variables and the default email template of the secure message notification containing a link which the Webmail users can click to read the message.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-pull-message
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-push-message

Use this sub-command to configure the variables and the default email template of the secure message notification with an attachment containing the secure message.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-push-message
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-user-register-done

Use this sub-command to configure the variables and the default email template of the IBE user registration notification.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-user-register-done
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-wread-notif

Use this sub-command to configure the variables and the default email template of the IBE “read” notification which is the first time the message is read.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-wread-notif
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-wunread-rcpt

Use this sub-command to configure the variables and the default email template of the IBE “unread” notification to the recipient when a mail remains unread for a period of time.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-wunread-rcpt
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

ibe-notify-wunread-sender

Use this sub-command to configure the variables and the default email template of the IBE “unread” notification to the sender when a mail remains unread for a period of time.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit ibe-notify-wread-notif
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the notification.	
html-body <string>	Enter the replacement message for the notification email body in HTML code.	
subject <string>	Enter the replacement message for the subject field of the notification.	
text-body <string>	Enter the replacement message for the notification email body in text format.	

log-report

Use this sub-command to configure the variables and the default content of the FortiMail log report.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit log-report
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set env-from <string>
      set from <string>
      set html-body <string>
      set subject <string>
      set text-body <string>
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%WARNING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%WARNING%% can be Disclaimer.	
env-from <string>	Enter the replacement message for the email Envelope From field.	
from <string>	Enter the replacement message for the email From field.	
html-body <string>	Enter the replacement email body in HTML format.	
subject <string>	Enter the replacement message for the email Subject header.	
text-body <string>	Enter the replacement email body in text format.	

login-disclaimer

Use this sub-command to configure the variables and the default content of the FortiMail system login disclaimer.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit login-disclaimer
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%WARNING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%WARNING%% can be Disclaimer.	
content <string>	Enter the replacement message for the login disclaimer.	
format {html multiline text}	Select the format for the login disclaimer.	html

reject-content-attachment

Use this sub-command to configure the variables and the default content of the attachment filtering message. This message is sent when an email is rejected for containing banned attachments.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-content-attachment
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	

Variable	Description	Default
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the attachment filtering message.	
format {html multiline text}	Select the format for the attachment filtering message.	html

reject-content-message

Use this sub-command to configure the variables and the default content of the content filtering message. This message is sent when an email is rejected for containing sensitive content.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-content-message
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the content filtering message.	
format {html multiline text}	Select the format for the content filtering message.	html

reject-delivery

Use this sub-command to configure the variables and the default content of the message delivery failure message.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-delivery
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the delivery failure message.	
format {html multiline text}	Select the format for the delivery failure message.	html

reject-endpoint-reputation

Use this sub-command to configure the variables and the default content of the content filtering message. This message is sent when an email is rejected for carrier endpoint reputation check.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-endpoint-reputation
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	

Variable	Description	Default
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Endpoint.	
content <string>	Enter the replacement message for the content filtering message.	
format {html multiline text}	Select the format for the content filtering message.	html

reject-spam

Use this sub-command to configure the variables and the default content of the spam message. This message is sent when an email is rejected for being detected as spam.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-spam
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the spam message.	
format {html multiline text}	Select the format for the spam message.	html

reject-virus-message

Use this sub-command to configure the variables and the default content of the virus message. This message is sent when an email is rejected for being infected with virus.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-virus-message
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the virus message.	
format {html multiline text}	Select the format for the virus message.	html

reject-virus-suspicious

Use this sub-command to configure the variables and the default content of the suspicious message. This message is sent when an email is rejected for containing suspicious components.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit reject-virus-suspicious
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECTION%%.	
content	Enter the content for the variable.	

Variable	Description	Default
display-name	Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice.	
content <string>	Enter the replacement message for the suspicious message.	
format {html multiline text}	Select the format for the suspicious message.	html

replace-content-attachment

Use this sub-command to create the variables for and replace the default content of the attachment filtering message. This message is sent when the attachment of an email is blocked.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit replace-content-attachment
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%BLOCK%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%BLOCK%% can be Notice.	
content <string>	Enter the replacement message for the attachment filtering message.	
format {html multiline text}	Select the format for the attachment filtering message.	html

replace-content-body

Use this sub-command to create the variables for and replace the default body of the content filtering message. This message is sent when an email is rejected for containing corporate sensitive data.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit replace-content-body
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECT%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%REJECT%% can be Notice.	
content <string>	Enter the replacement message for the body of the content filtering message.	
format {html multiline text}	Select the format for the body of the content filtering message.	html

replace-content-subject

Use this sub-command to create the variables for and replace the default subject of the content filtering message. This message is sent when an email is rejected for containing corporate sensitive data.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit replace-content-subject
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%REJECT%%.	
content	Enter the content for the variable.	

Variable	Description	Default
display-name	Enter the display name for the variable. For example, the display name for %%REJECT%% can be Notice.	
content <string>	Enter the replacement message for the subject of the content filtering message.	
format {html multiline text}	Select the format for the subject of content filtering message.	html

replace-virus-message

Use this sub-command to configure the variables and the default replacement message for infected email attachments. This message is sent when an email's attachment is removed for being infected with a virus.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit replace-virus-message
  config variable
    edit <name>
      set content
      set display-name
  config message
    edit default
      set content <string>
      set format {html | multiline | text}
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%WARNING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice.	
content <string>	Enter the replacement message for infected email attachments.	
format {html multiline text}	Select the format for the replacement message of infected email attachments.	html

replace-virus-suspicious

Use this sub-command to configure the variables and the default replacement message for suspicious email attachments. This message is sent when an email's attachment is removed for containing suspicious components.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit replace-virus-suspicious
  config variable
    edit <name>
      set content
      set display-name
    config message
      edit default
        set content <string>
        set format {html | multiline | text}
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%WARNING%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice.	
content <string>	Enter the replacement message for suspicious email attachments.	
format {html multiline text}	Select the format for the replacement message of suspicious email attachments.	html

report-quarantine-summary

Use this sub-command to configure the variables and the default email template of quarantine summary.

Syntax

This sub-command is available from within the command `customized-message`.

```
edit report-quarantine-summary
  config variable
    edit <name>
      set content
      set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the quarantine summary.	
html-body <string>	Enter the replacement message for the email body of the quarantine summary in HTML code.	
subject <string>	Enter the replacement message for the subject field of the quarantine summary.	
text-body <string>	Enter the replacement message for the email body of the quarantine summary in text format.	

dlp scan-rules

Use these commands to prevent sensitive data from leaving your network.

Syntax

Text.

```

config dlp scan-rules
  edit <rule_name>
    config_conditions
      edit <condition_id_>
        set attribute
        set file-pattern
        set group-type
        set ldap-profile
        set operator
        set sensitive-data
        set value
      config_exceptions
        edit <exception_id>
          set attribute
          set file-pattern
          set group-type
          set ldap-profile
          set operator
          set sensitive-data
          set value
        end
    end
  end

```

Variable	Description	Default
<rule_name>	Enter a descriptive name for the rule.	No default.
conditions	Select either Match all conditions or Match any condition.	

Variable	Description	Default
exceptions	Email matching the exceptions will not be scanned.	
attribute	Enter a descriptive name.	
file-pattern	Enter a filename pattern to restrict fingerprinting to only those files that match the pattern.	
group-type	Set whether the group is local or ldap	
ldap-profile	Select your ldap profile.	
operator	Enter the scan conditions (contains/doesn't contain)	
sensitive-data	Enter a predefined sensitive information term.	
value	Enter the attribute value in string format.	

domain

Use these commands to configure a protected domain.

For more information on protected domains and when they are required, see the [FortiMail Administration Guide](#).

Syntax

This command contains many sub-commands. Each sub-command, linked below, is documented in subsequent sections.

```

config domain
  edit <domain_name>
    config customized-message...
    config domain-setting...
    config policy recipient...
    config profile antispam...
    config profile antispam-action...
    config profile antivirus...
    config profile antivirus-action
    config profile authentication...
    config profile content...
    config profile content-action...
    config profile resource...
    config user mail...
    config user group...
  next
end

```

Variable	Description	Default
<domain_name>	Type the fully qualified domain name (FQDN) of the protected domain. For example, to protect email addresses ending in “@example.com”, type <code>example.com</code> .	No default.

Related topics

- [config customized-message](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config customized-message

Use this sub-command to configure the variables and the default email template of quarantine summary of a protected domain.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config customized-message
  edit report-quarantine-summary
    config variable
      edit <name>
        set content
        set display-name
    config email-template
      edit default
        set from <string>
        set html-body <string>
        set subject <string>
        set text-body <string>
      end
    end
  end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the quarantine summary.	
html-body <string>	Enter the replacement message for the email body of the quarantine summary in HTML code.	

Variable	Description	Default
subject <string>	Enter the replacement message for the <code>subject</code> field of the quarantine summary.	
text-body <string>	Enter the replacement message for the email body of the quarantine summary in text format.	

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config domain-setting

Use this sub-command to configure the basic settings of a protected domain.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config domain-setting
  set addressbook {domain | none | system}
  set bypass-bounce-verification {enable | disable}
  set fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>}
  set fallback-port <port_int>
  set fallback-use-smtps {enable | disable}
  set global-bayesian {enable | disable}
  set greeting-with-host-name {domainname | hostname | othername}
  set host <host_name>
  set ip-pool <pool_name>
  set ip-pool-direction {outgoing | incoming | both}
  set is-sub-domain {enable | disable}
  set ldap-asav-profile <ldap-profile_name>
  set ldap-asav-status {enable | disable}
  set ldap-domain-routing-port <port_int>
  set ldap-domain-routing-profile <ldap-profile_name>
  set ldap-domain-routing-smtps {enable | disable}
  set ldap-groupowner-profile <ldap-profile_name>
  set ldap-routing-profile <ldap-profile_name>
  set ldap-routing-status {enable | disable}
  set ldap-user-profile <profile_name>
  set max-message-size <limit_int>
  set other-helo-greeting <string>
  set port <smtp-port_int>
  set quarantine-report-schedule-status {enable | disable}
  set quarantine-report-status {enable | disable}
  set quarantine-report-to-alt {enable | disable}
  set quarantine-report-to-alt-addr <recipient_email>
  set quarantine-report-to-individual {enable | disable}
  set quarantine-report-to-ldap-groupowner {enable | disable}
  set recipient-verification {disable | ldap | smtp}
  set recipient-verification-background {disable | ldap | smtp}
  set relay-type {host | ip-pool | ldap-domain-routing | mx-lookup |
    mx-lookup-alt-domain}
  set remove-outgoing-received-header {enable | disable}
  set sender-addr-rate-ctrl-max-msgs <integer>
  set sender-addr-rate-ctrl-max-msgs-state {enable | disable}
  set sender-addr-rate-ctrl-max-size <integer>
  set sender-addr-rate-ctrl-max-size-state {enable | disable}
  set sender-addr-rate-ctrl-state {enable | disable}
  set smtp-recipient-verification-command {rcpt | vrfy}
  set smtp-recipient-verification-accept-reply-string
    <accept_string>
  set tp-hidden {no | yes}
  set tp-server-on-port <port_int>
  set tp-use-domain-mta {yes | no}
```

```

set use-stmps {enable | disable}
set webmail-language <language_name>
set web-theme {IndigoDarkBlue | RedGrey | Standard |
               Use-System-Settings}
end

```

Variable	Description	Default
addressbook {domain none system} (server mode only)	Add newly created mail user to system address book, domain address book or not.	domain
bypass-bounce-verification {enable disable}	Enable to omit bounce address tag verification of email incoming to this protected domain. This bypass does not omit bounce address tagging of outgoing email.	disable
fallback-host {<smtp-server_fqdn> <smtp-server_ipv4>} (transparent mode and gateway mode only)	Enter the fully qualified domain name (FQDN) or IP address of the secondary SMTP server for this protected domain. This SMTP server will be used if the primary SMTP server is unreachable.	No default.
fallback-port <port_int> (transparent mode and gateway mode only)	Enter the port number on which the failover SMTP server listens. If you enable Use SMTPS, Port automatically changes to the default port number for SMTPS, but can still be customized. The default SMTP port number is 25; the default SMTPS port number is 465.	25
fallback-use-smtps {enable disable} (transparent mode and gateway mode only)	Enable to use SMTPS for connections originating from or destined for this protected server.	disable
global-bayesian {enable disable}	Enable to use the global Bayesian database instead of the Bayesian database for this protected domain. If you do not need the Bayesian database to be specific to the protected domain, you may want to use the global Bayesian database instead in order to simplify database maintenance and training. Disable to use the per-domain Bayesian database. This option does not apply if you have enabled use of personal Bayesian databases in an incoming antispam profile, and if the personal Bayesian database is mature. Instead, the FortiMail unit will use the personal Bayesian database.	disable

Variable	Description	Default
greeting-with-host-name {domainname host-name othername}	<p>Specify how the FortiMail unit will identify itself during the HELO or EHLO greeting of outgoing SMTP connections that it initiates.</p> <p><i>domainname</i>: The FortiMail unit will identify itself using the domain name for this protected domain.</p> <p>If the FortiMail unit will handle internal email messages (those for which both the sender and recipient addresses in the envelope contain the domain name of the protected domain), to use this option, you must also configure your protected SMTP server to use its host name for SMTP greetings. Failure to do this will result in dropped SMTP sessions, as both the FortiMail unit and the protected SMTP server will be using the same domain name when greeting each other.</p> <p><i>hostname</i>: The FortiMail unit will identify itself using its own host name.</p> <p>By default, the FortiMail unit uses the domain name of the protected domain. If your FortiMail unit is protecting multiple domains and using IP pool addresses, select to use the system host name instead. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.</p> <p><i>othername</i>: If you select this option, another command <code>set other-helo-greeting <string></code> will appear, allowing you enter a name other than the domain name or host name, for the HELO/EHELO greeting.</p>	hostname
host <host_name> (transparent mode and gateway mode only)	<p>The host name or IP address and port number of the mail exchanger (MX) for this protected domain.</p> <p>If Relay Type is MX Record (this domain) or MX Record (alternative domain), this information is determined dynamically by querying the MX record of the DNS server, and this field will be empty.</p>	No default.

Variable	Description	Default
ip-pool <pool_name>	<p>You can use a pool of IP addresses as the source IP address when sending email from this domain, or as the destination IP address when receiving email destined to this domain, or as both the source and destination IP addresses.</p> <ul style="list-style-type: none"> If you want to use the IP pool as the source IP address for this protected domain, according to the sender's email address in the envelope (MAIL FROM:), select the IP pool to use and select <i>outgoing</i> as the ip-pool-direction. If you want to use the IP pool as the destination IP address (virtual host) for this protected domain, according to the recipient's email address in the envelope (RCPT TO:), select the IP pool to use and select <i>incoming</i> as the ip-pool-direction. You must also configure the MX record to direct email to the IP pool addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well. If you want to use the IP pool as both the destination and source IP address, select the IP pool to use and select <i>Both</i> as the ip-pool-direction. <p>Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.</p>	No default.
ip-pool-direction {outgoing incoming both}	<p>Sets the direction for the ip-pool option. See description above.</p> <p>This option is only available after you configure the ip-pool option.</p>	
is-sub-domain {enable disable }	<p>Enable to indicate the protected domain you are creating is a subdomain of an existing protected domain, then also configure Main domain.</p> <p>Subdomains, like their parent protected domains, can be selected when configuring policies specific to that subdomain. Unlike top-level protected domains, however, subdomains will be displayed as grouped under the parent protected domain when viewing the list of protected domains.</p> <p>This option is available only when another protected domain exists to select as the parent domain.</p>	disable
ldap-asav-profile <ldap-profile_name>	Specify the name of an LDAP profile which you have enabled and configured.	No default.
ldap-asav-status {enable disable }	Enable to query an LDAP server for an email user's preferences to enable or disable antispam and/or antivirus processing for email messages destined for them.	disable

Variable	Description	Default
ldap-domain-routing-port <port_int>	<p>Enter the port number on which the SMTP servers in the LDAP profile listen.</p> <p>If you enable <code>ldap-domain-routing-smtps</code>, this setting automatically changes to the default port number for SMTPS, but can still be customized.</p> <p>The default SMTP port number is 25; the default SMTPS port number is 465.</p> <p>This option is valid when <code>relay-type</code> is <code>ldap-domain-routing</code>.</p>	25
ldap-domain-routing-profile <ldap-profile_name>	<p>Select the name of the LDAP profile that has the FQDN or IP address of the SMTP server you want to query. Also configure <GUIElement><code>ldap-domain-routing-port</code> <port_int> and <GUIElement><code>ldap-domain-routing-smtps</code> {enable disable}.</p> <p>This option is valid when <code>relay-type</code> is set to <code>ldap-domain-routing</code>.</p>	
ldap-domain-routing-smtps {enable disable}	<p>Enable to use SMTPS for connections originating from or destined for this protected server.</p> <p>This option is valid when <code>relay-type</code> is <code>ldap-domain-routing</code>.</p>	disable
ldap-groupowner-profile <ldap-profile_name>	Select an LDAP profile to send the quarantine report to a group owner, rather than individual recipients.	No default.
ldap-routing-profile <ldap-profile_name>	Select an LDAP profile for mail routing.	No default.
ldap-routing-status {enable disable }	Enable/disable LDAP mail routing.	disable
ldap-user-profile <profile_name>	Select the name of an LDAP profile in which you have configured, enabling you to authenticate email users and expand alias email addresses or replace one email address with another by using an LDAP query to retrieve alias members.	No default.
max-message-size <limit_int>	<p>Enable then type the limit in kilobytes (KB) of the message size. Email messages over the threshold size are rejected.</p> <p>Note: If both this option and <code>limit-max-message-size</code> <limit_int> in the session profile are enabled, email size will be limited to whichever size is smaller.</p>	10240
other-helo-greeting <string>	After you set the <code>greeting-with-hostname</code> to <code>othername</code> , use this command to specify the name to use for HELO/EHELO greeting.	

Variable	Description	Default
port <smtp-port_int> (transparent mode and gateway mode only)	Set the SMTP port number of the mail server.	25
quarantine-report -schedule-status {enable disable }	Enable or disable domain-level quarantine report schedule setting. The quarantine report settings for a protected domain are a subset of the system-wide quarantine report settings. For example, if the system settings for schedule include only Monday and Thursday, when you are setting the schedule for the quarantine reports of the protected domain, you will only be able to select either Monday or Thursday.	disable
quarantine-report -status {enable disable }	Enable or disable domain-level quarantine report.	disable
quarantine-report -to-alt {enable disable }	Enable or disable sending domain-level quarantine report to a recipient other than the individual recipients or group owner. For example, you might delegate quarantine reports by sending them to an administrator whose email address is not locally deliverable to the protected domain, such as admin@lab.example.com.	disable
quarantine-report -to-alt-addr <recipient_email>	Enter the recipient's email address.	No default.
quarantine-report -to-individual {enable disable }	Enable to send quarantine reports to all recipients.	enable
quarantine-report -to-ldap-groupowner {enable disable }	Enable to send quarantine reports to the LDAP group owner of the specified LDAP profile.	disable

Variable	Description	Default
recipient-verification {disable ldap smtp}	<p>Select a method of confirming that the recipient email address in the message envelope (RCPT TO:) corresponds to an email user account that actually exists on the protected email server. If the recipient address is invalid, the FortiMail unit will reject the email. This prevents quarantine email messages for non-existent accounts, thereby conserving quarantine hard disk space.</p> <ul style="list-style-type: none"> disable: Do not verify that the recipient address is an email user account that actually exists. smtp: Query the SMTP server using the SMTP RCPT command to verify that the recipient address is an email user account that actually exists. You can also choose to use the SMTP VRFY command to do the verification. This feature is available on the GUI when you create a domain. If you want to query an SMTP server other than the one you have defined as the protected SMTP server, also enable Use alternative server, then enter the IP address or FQDN of the server in the field next to it. Also configure Port with the TCP port number on which the SMTP server listens, and enable Use SMTPS if you want to use SMTPS for recipient address verification connections with the server. ldap: Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. <p>Note: This option can cause a performance impact that may be noticeable during peak traffic times. For a lesser performance impact, you can alternatively periodically automatically remove quarantined email messages for invalid email user accounts, rather than actively preventing them during each email message.</p> <p>Note: Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or the periodic removal of invalid quarantine accounts.</p>	disable

Variable	Description	Default
<code>recipient-verification-background {disable ldap smtp}</code>	<p>Select a method by which to periodically remove quarantined spam for which an email user account does not actually exist on the protected email server.</p> <ul style="list-style-type: none"> <code>disable</code>: Do not verify that the recipient address is an email user account that actually exists. <code>smtp</code>: Query the SMTP server to verify that the recipient address is an email user account that actually exists. <code>ldap</code>: Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. If you select either Use SMTP server or Use LDAP server, at 4:00 AM daily (unless configured for another time, using the CLI), the FortiMail unit queries the server to verify the existence of email user accounts. If an email user account does not currently exist, the FortiMail unit removes all spam quarantined for that email user account. <p>Note: If you have also enabled <code>recipient-verification</code>, the FortiMail unit is prevented from forming quarantine accounts for email user accounts that do not really exist on the protected email server. In that case, invalid quarantine accounts are never formed, and this option may not be necessary, except when you delete email user accounts on the protected email server. If this is the case, you can improve the performance of the FortiMail unit by disabling this option.</p> <p>Note: Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or verification of recipient addresses.</p>	No default.

Variable	Description	Default
<pre>relay-type {host ip-pool ldap-domain-routing mx-lookup mx-lookup-alt-domain}</pre> <p>(transparent mode and gateway mode only)</p>	<p>Select from one of the following methods of defining which SMTP server will receive email from the FortiMail unit that is destined for the protected domain:</p> <ul style="list-style-type: none"> host: Configure the connection to one protected SMTP server or, if any, one fallback. ldap-domain-routing: Query the LDAP server for the FQDN or IP address of the SMTP server. For more information about domain lookup, see “domain-query <query_str>” on page 219. mx-lookup: Query the DNS server’s MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. mx-lookup-alt-domain: Query the DNS server’s MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. ip-pool: Configure the connection to rotate among one or many protected SMTP servers. <p>Note: If an MX option is used, you may also be required to configure the FortiMail unit to use a private DNS server whose MX and/or A records differ from that of a public DNS server. Requirements vary by the topology of your network and by the operating mode of the FortiMail unit.</p> <ul style="list-style-type: none"> Gateway mode: A private DNS server is required. On the private DNS server, configure the MX record with the FQDN of the SMTP server that you are protecting for this domain, causing the FortiMail unit to route email to the protected SMTP server. This is different from how a public DNS server should be configured for that domain name, where the MX record usually should contain the FQDN of the FortiMail unit itself, causing external SMTP servers to route email through the FortiMail unit. Additionally, if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall, on the private DNS server, configure the protected SMTP server’s A record with its private IP address, while on the public DNS server, configure the FortiMail unit’s A record with its public IP address. Transparent mode: A private DNS server is required if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall. On the private DNS server, configure the protected SMTP server’s A record with its private IP address. On the public DNS server, configure the protected SMTP server’s A record with its public IP address. Do not modify the MX record. 	host

Variable	Description	Default
<code>remove-outgoing-received-header</code> {enable disable}	<p>Enable to remove the <code>Received:</code> message headers from email whose:</p> <ul style="list-style-type: none"> • sender email address belongs to this protected domain • recipient email address is outgoing (that is, does not belong to this protected domain); if there are multiple recipients, only the first recipient's email address is used to determine whether an email is outgoing <p>You can alternatively remove this header from any matching email using session profiles.</p>	disable
<code>sender-addr-rate-ctrl-max-msgs</code> <integer>	<p>Enter the maximum number of messages per sender address per half an hour.</p> <p>This feature is only available for FortiMail 3000D/VM16 and higher platform.</p>	30
<code>sender-addr-rate-ctrl-max-msgs-state</code> {enable disable}	<p>Enable the option of maximum number of messages per sender address per half an hour.</p> <p>This feature is only available for FortiMail 3000D/VM16 and higher platform.</p>	disable
<code>sender-addr-rate-ctrl-max-size</code> <integer>	<p>Enter the maximum number of megabytes per sender per half an hour.</p> <p>This feature is only available for FortiMail 3000D/VM16 and higher platform.</p>	100
<code>sender-addr-rate-ctrl-max-size-state</code> {enable disable}	<p>Enable the option of maximum number of megabytes per sender per half an hour.</p> <p>This feature is only available for FortiMail 3000D/VM16 and higher platform.</p>	disable
<code>sender-addr-rate-ctrl-state</code> {enable disable}	<p>Enable sender address rate control per sender email address.</p> <p>This feature is only available for FortiMail 3000D/VM16 and higher platform.</p>	disable
<code>smtp-recipient-verification-command</code> {rcpt vrfy} (transparent mode and gateway mode only)	<p>Specify the command that the FortiMail unit uses to query the SMTP server to verify that the recipient address is an email user account that actually exists. The default command that the FortiMail unit uses is <code>rcpt</code>. For information about recipient verification, see recipient-verification {disable ldap smtp}.</p> <p>This option is only available after you select <code>smtp</code> in <code>recipient-verification</code>.</p>	rcpt

Variable	Description	Default
smtp-recipient-verification-accept-reply-string <accept_string> (transparent mode and gateway mode only)	<p>When FortiMail queries the SMTP server for recipient verification:</p> <ul style="list-style-type: none"> • If the reply code of the VRFY command is 2xx, the recipient exists. • If the reply code is non-2xx, FortiMail will try to match the accept string you specified with the reply string. If the strings match, the recipient exists. • Otherwise, the recipient is unknown. <p>For example, if the recipient is a group or mailing list, FortiMail will receive a 550 error code and a reply string. Depending on what reply string you get, you can specify a string to match the reply string.</p> <p>For example, if the recipient is marketing@example.com, the reply string might say something like "marketing@example.com is a group". In this case, if you specify "is a group" as the accept string and thus this string matches the string or part of the string in the reply string, FortiMail will deem the query successful and pass the email.</p> <p>This command is available only when you set SMTP-recipient-verification-command to vrfy.</p>	

Variable	Description	Default
tp-hidden {no yes} (transparent mode only)	<p>Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in:</p> <ul style="list-style-type: none"> the SMTP greeting (HELO/EHLO) in the envelope and in the Received: message headers of email messages the IP addresses in the IP header <p>This masks the existence of the FortiMail unit to the protected SMTP server.</p> <p>Disable to replace the SMTP client's IP address or domain name with that of the FortiMail unit.</p> <p>For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in bold):</p> <p>Received: from 192.168.1.1 (EHLO 172.16.1.1) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800</p> <p>Received: from smtpa ([172.16.1.2]) by [172.16.1.1] with SMTP id KAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT</p> <p>But if the option is disabled, the message headers would contain:</p> <p>Received: from 192.168.1.1 (EHLO fortimail.example.com) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800</p> <p>Received: from smtpa ([172.16.1.2]) by fortimail.example.com with SMTP id KAOFJI4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT</p>	no
tp-server-on-port <port_int> (transparent mode only)	<p>Select the network interface (physical port) to which the protected SMTP server is connected.</p> <p>Note: Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface.</p>	0

Variable	Description	Default
<code>tp-use-domain-mta</code> <code>{yes no}</code> (transparent mode only)	<p>Enable to proxy SMTP clients' incoming connections when sending outgoing email messages via the protected SMTP server.</p> <p>For example, if the protected domain example.com has the SMTP server 192.168.1.1, and an SMTP client for user1@example.com connects to it to send email to user2@external.example.net, enabling this option would cause the FortiMail unit to proxy the connection through to the protected SMTP server.</p> <p>Disable to relay email using the built-in MTA to either the defined SMTP relay, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (RCPT TO:) domain. The email may not actually travel through the protected SMTP server, even though it was the relay originally specified by the SMTP client.</p> <p>This option does not affect incoming connections containing incoming email messages, which will always be handled by the built-in MTA.</p> <p>Note: This option will be ignored for email that matches an antispam or content profile where you have enabled <code>alternate-host {<relay_fqdn> <relay_ipv4>}</code>.</p>	no
<code>use-stmps</code> <code>{enable disable}</code>	Enable to use SMTPS to relay email to the mail server.	disable
<code>webmail-language</code> <code><language_name></code>	Select the language that the FortiMail unit will to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same language as the web-based manager.	No default.
<code>web-theme</code> <code>{IndigoDarkBlue RedGrey Standard Use-System-Settings}</code>	Select the display theme that the FortiMail unit will to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same display theme as the web-based manager.	Use-System-Settings

Related topics

- [dlp scan-rules](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)
- [debug application starttls](#)

config policy recipient

Use this sub-command to configure a recipient-based policy for a protected domain.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config policy recipient
  edit <policy_index>
    set auth-access-options {pop3 smtp-auth smtp-diff-identity web}
    set certificate-required {yes | no}
    set comment
    set direction
    set pkiauth {enable | disable}
    set pkiuser <user_name>
    set profile-antispam <antispam_name>
    set profile-antivirus <antivirus_name>
    set profile-auth-type {imap | local | ldap | pop3 | smtp |
      radius}
    set profile-content <profile_name>
    set profile-dlp
    set profile-resource <profile_name>
    set profile-ldap <profile_name>
    set recipient-name <name_str>
    set recipient-type {ldap-group | local-group | user}
    set sender-domain <domain_name>
    set sender-name <local-part_str>
    set sender-type {ldap-group | local-group | user}
    set smtp-diff-identity
    set smtp-diff-identity
    set smtp-diff-identity-ldap-profile
    set status {enable | disable}
  next
end
```

Variable	Description	Default
<policy_index>	Type the index number of the policy. To view a list of existing entries, enter a question mark (?).	No default.
auth-access-options {pop3 smtp-auth smtp-diff-identity web}	Type one or more of the following: <ul style="list-style-type: none"> smtp-diff-identity: Allow email when the SMTP client authenticates with a different user name than the one that appears in the envelope's sender email address. You must also enter <code>smtpauth</code> for this option to have any effect. web: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine. pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine. smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. Note: Entering this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication. 	No default.
certificate-required {yes no} (transparent and gateway mode only)	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enable this option.	no
comment	Enter a comment for the recipient policy	
direction		
pkiauth {enable disable} (transparent and gateway mode only)	Enable if you want to allow email users to log in to their per-recipient spam quarantine by presenting a certificate rather than a user name and password.	disable
pkiuser <user_name> (transparent and gateway mode only)	Enter the name of the PKI user entry, or select a user you defined before. This is not required to be the same as the administrator or email user's account name, although you may find it helpful to do so. For example, you might have an administrator account named <code>admin1</code> . You might therefore find it most straightforward to also name the PKI user <code>admin1</code> , making it easy to remember which account you intended to use these PKI settings.	No default.
profile-antispam <antispam_name>	Select a antispam profile that you want to apply to the policy.	No default.
profile-antivirus <antivirus_name>	Select an antivirus profile that you want to apply to the policy.	No default.

Variable	Description	Default
profile-auth-type {imap local ldap pop3 smtp radius}	If you want email users to be able to authenticate using an external authentication server, first specify the profile type (SMTP, POP3, IMAP, RADIUS, or LDAP), then specify which profile to use. For example: set profile-auth-type ldap set profile-auth-ldap ldap_profile1	No default.
profile-auth-imap <imap_name>	Type the name of an IMAP authentication profile. This command is applicable only if you have enabled use of an IMAP authentication profile using profile-auth-type {imap local ldap pop3 smtp radius}.	No default.
profile-auth-ldap <ldap_name>	Type the name of an LDAP authentication profile. This command is applicable only if you have enabled use of an LDAP authentication profile using profile-auth-type {imap local ldap pop3 smtp radius}.	No default.
profile-auth-pop3 <pop3_name>	Type the name of a POP3 authentication profile. This command is applicable only if you have enabled use of a POP3 authentication profile using profile-auth-type {imap local ldap pop3 smtp radius}.	No default.
profile-auth-smtp <smtp_name>	Type the name of an SMTP authentication profile. This command is applicable only if you have enabled use of an SMTP authentication profile using profile-auth-type {imap local ldap pop3 smtp radius}.	No default.
profile-auth-radius <radius_name>	Type the name of a RADIUS authentication profile. This command is applicable only if you have enabled use of a RADIUS authentication profile using profile-auth-type {imap local ldap pop3 smtp radius}.	No default.
profile-content <profile_name>	Select which content profile you want to apply to the policy.	No default.
profile-dlp		
profile-resource <profile_name>	Select which resource profile you want to apply to the policy. This option is only available in server mode.	No default.
profile-ldap <profile_name>	If you set the recipient type as "ldap-group", you can select an LDAP profile.	
recipient-name <name_str>	Enter the local part of the recipient email address or a pattern with wild cards.	No default.

Variable	Description	Default
recipient-type {ldap-group local-group user}	<p>Select one of the following ways to define recipient (RCPT TO:) email addresses that match this policy. This setting applies to the incoming policies only.</p> <ul style="list-style-type: none"> • user: Select this option and then use the above command to enter the local part of the recipient email address. • local-group: Select this option and then specify the local group under this domain. • ldap-group: Select this option and then select an LDAP profile. 	user
sender-domain <domain_name>	Enter the domain part of the sender email address. For example, example.com.	
sender-name <local-part_str>	Enter the local part of the sender email address. For example, user1.	
sender-type {ldap-group local-group user}	<p>Select one of the following ways to define which sender (MAIL FROM:) email addresses match this policy.</p> <ul style="list-style-type: none"> • user: Select this option and then use the above command to enter the local part of the sender email address. • local-group: Select this option and then specify the local group under this domain. • ldap-group: Select this option and then select an LDAP profile. <p>Note: This setting applies to the outgoing policies only.</p>	user
smtp-diff-identity	Rejects different smtp sender identity.	
smtp-diff-identity-ldap	Verify smtp sender identity with LDAP for authenticated email.	
smtp-diff-identity-ldap-profile	Ldap profile for smtp sender identity verification.	
status {enable disable }	Enable or disable the policy.	enable

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile antispam

Use this sub-command to configure antispam profiles for a protected domain. To configure system-wide antispam profiles, use [“profile antispam” on page 166](#).

FortiMail units can use various methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, Bayesian scanning, and heuristic scanning. Antispam profiles contain settings for these features that you may want to vary by policy. Depending on the feature, before you configure antispam policies, you may need to enable the feature or configure its system-wide settings.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile antispam
    edit <profile_name>
        set (options)
        config (options)
```

For more information about the `set` and `config` options, see [“profile antispam” on page 166](#).

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile antispam-action

Use this sub-command to define antispam action profiles.

Antispam action profiles define one or more things that the FortiMail unit should do if the antispam profile determines that an email is spam.

For example, you might have configured an antispam action profile named `quar_and_tag_profile`, which both tags the subject line and quarantines email detected to be spam. In general, all antispam profiles using `quar_and_tag_profile` will therefore both quarantine and tag spam. However, you have decided that email that does not pass the dictionary scan is always spam and should be rejected so that it does not consume quarantine disk space. Therefore, for the antispam profiles that apply a dictionary scan, you would override the action profile's default action by configuring and selecting a second action profile, named `rejection_profile`, which rejects such email.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile antispam-action
  edit <profile_name>
    set action {discard | none | quarantine | quarantine-review |
      reject | rewrite-rcpt}
    set alternate-host <name/ip_string>
    set alternate-host-status {enable | disable}
    set archive-account <name_string>
    set archive-status {enable | disable}
    set bcc-addr <email_address>
    set bcc-status {enable | disable}
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set notification-profile <name_string>
    set notification-status {enable | disable}
    set release-through-email {enable | disable}
    set release-through-web {enable | disable}
    set release-auto-whitelist {enable | disable}
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
    set subject-tagging-status {enable | disable}
    set subject-tagging-text <tag_str>
  next
end
```

Variable	Description	Default
<code><profile_name></code>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
<code>action {discard none quarantine quarantine-review reject rewrite-rcpt}</code>	Type an action for the profile. <ul style="list-style-type: none"> <code>discard</code>: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. <code>none</code>: Apply any configured header or subject line tags, if any. <code>quarantine</code>: Enter to redirect spam to the per-recipient quarantine. For more information, see the FortiMail Administration Guide. This option is available only for incoming profiles. <code>quarantine-review</code>: Enter to redirect spam to the system quarantine. For more information, see the FortiMail Administration Guide. <code>reject</code>: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. <code>rewrite-rcpt</code>: Enter to change the recipient address of any email message detected as spam. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). 	none
<code>alternate-host</code> <code><name/ip_string></code>	Type the name or IP address of the SMTP server or relay where you want to route the email to. If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile.	No default.
<code>alternate-host-status</code> <code>{enable disable}</code>	Enable to route the email to a specific SMTP server or relay.	disable
<code>archive-account</code> <code><name_string></code>	Type the name of the archive account for archiving the email.	No default.
<code>archive-status</code> <code>{enable disable}</code>	Enable to send the email to an archiving account.	disable
<code>bcc-addr</code> <code><email_address></code>	Type the BCC recipient email addresses for sending a blind carbon copy (BCC) of the email.	No default.
<code>bcc-status</code> <code>{enable disable}</code>	Enable to send a blind carbon copy (BCC) of the email.	disable

Variable	Description	Default
header-insertion-name <name_str>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <p>X-Custom-Header: Detected as spam by profile 22.</p> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-value <header_str>.</p>	
header-insertion-status {enable disable }	<p>Enable to add a message header to detected spam.</p> <p>See header-insertion-value <header_str>.</p>	disable
header-insertion-value <header_str>	<p>Enter the message header value.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <p>X-Custom-Header: Detected as spam by profile 22.</p> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-name <name_str>.</p>	
notification-profile <name_string>	Type the name of the notification profile used for sending notifications.	No default.
notification-status {enable disable }	Enable sending notifications using a notification profile.	disable
release-through-email {enable disable }	Enable to allow email users to remotely release email from the quarantine by sending email to quarantine control account email addresses. For more information, see the FortiMail Administration Guide .	disable

Variable	Description	Default
release-through-web {enable disable}	Enable to allow email users to remotely release email from the quarantine by selecting the <i>Release</i> link in a quarantine report. For more information, see the FortiMail Administration Guide .	disable
release-auto-whitelist {enable disable}	Enable to, when an email user releases an email from the quarantine, automatically add the sender email address of the quarantined email to the email user's personal white list <i>if</i> the option is also enabled in the email user's preferences. Email users' preferences can be configured from both the <i>Preferences</i> tab of FortiMail webmail and from the web-based manager. For more information, see the FortiMail Administration Guide .	disable
rewrite-rcpt-local-type {none prefix replace suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam. <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>. 	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none prefix replace suffix} .	
rewrite-rcpt-domain-type {none-prefix replace suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam. <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. 	none
rewrite-rcpt-domain-value <value_str>	Type the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix replace suffix} .	
subject-tagging-status {enable disable}	Enable to prepend text ("tag") defined using subject-tagging-text <tag_str> to the subject line on detected spam.	disable
subject-tagging-text <tag_str>	Enter the text that will appear in the subject line of the email, such as "[SPAM]". The FortiMail unit will prepend this text to the subject line of spam before forwarding it to the recipient.	

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile antivirus

Use this sub-command to create antivirus profiles that you can select in a policy in order to scan email for viruses.

If the FortiMail unit detects a virus, it replaces the infected file with a replacement message that notifies the email user the infected file has been removed. You can customize replacement messages. For more information, see the *FortiMail Administration Guide*.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile antivirus
  edit <profile_name>
    set action-default
      {predefined_av_discard | predefined_av_reject}
    set action-file-signature
    set action-heuristic
      {predefined_av_discard | predefined_av_reject}
    set action-outbreak
    set action-sandbox-high
    set action-sandbox-low
    set action-sandbox-virus
    set file-signature-check
    set grayware-scan
    set heuristic {enable | disable}
    set malware-outbreak-protection
    set sandbox-analysis
    set sandbox-analysis-uri
    set sandbox-scan-mode
    set scanner {enable | disable}
  next
end
```


Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	
action-default {predefined_av_discard predefined_av_reject}	Type a predefined action on infected email. predefined_av_discard: Accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client. predefined_av_reject: Reject infected email and reply to the SMTP client with SMTP reply code 550.	No default.
action-file-signature		
action-heuristic {predefined_av_discard predefined_av_reject}	Type a predefined heuristic scanning action on infected email. predefined_av_discard: Accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client. predefined_av_reject: Reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550.	No default.
action-outbreak		
action-sandbox-high		
action-sandbox-low		
action-sandbox-virus		
file-signature-check		
grayware-scan		
malware-outbreak-protection	Enable or disable realtime malware outbreak protection.	disable
heuristic {enable disable}	Enable to perform heuristic scanning for this profile.	disable
sandbox-analysis	Enable or disable sending suspicious attachment content to FortiSandbox for analysis.	disable
sandbox-analysis-uri	Enable or disable sending suspicious uri to FortiSandbox for analysis.	
sandbox-scan-mode	Enter how the email is handled by FortiSandBox	
scanner {enable disable}	Enable to perform antivirus scanning for this profile.	disable

Related topics

- [dlp scan-rules](#)

- config domain-setting
- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile authentication
- config profile content
- config profile content-action
- config user mail
- config user group

config profile antivirus-action

Use this sub-command to define antivirus action profiles.

Antivirus action profiles define one or more things that the FortiMail unit should do if the antivirus profile determines that an email is infected.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile antispam-action
  edit <profile_name>
    set action {discard | none | quarantine-review | reject |
      repackaging | repackaging-with-cmsg | replace-infected |
      rewrite-rcpt}
    set alternate-host <name/ip_string>
    set alternate-host-status {enable | disable}
    set bcc-addr <email_address>
    set bcc-status {enable | disable}
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set notification-profile <name_string>
    set notification-status {enable | disable}
    set subject-tagging-status {enable | disable}
    set subject-tagging-text <tag_str>
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
  next
end
```

Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
action {discard none quarantine-review reject repackage repackage-with-cmsg replace-infected rewrite-rcpt}	Type an action for the profile. <ul style="list-style-type: none"> discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. none: Apply any configured header or subject line tags, if any. quarantine-review: Enter to redirect infected email to the system quarantine. For more information, see the <i>FortiMail Administration Guide</i>. reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. repackage: Enter to repackage the email with original text content and the original email is wrapped as an attachment. repackage-with-cmsg: Enter to repackage the email with customized text content and the original email is wrapped as an attachment. replace-infected: Enter to replace infected or suspicious email body or attachments. rewrite-rcpt: Enter to change the recipient address of any email message detected as infected. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). If you enter this option, also configure <code>rewrite-rcpt-local-type {none prefix replace suffix}</code>, <code>rewrite-rcpt-local-value <value_str></code>, <code>rewrite-rcpt-domain-type {none-prefix replace suffix}</code>, and <code>rewrite-rcpt-domain-value <value_str></code>. 	none
alternate-host <name/ip_string>	Type the name or IP address of the SMTP server or relay where you want to route the email to. If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile.	No default.
alternate-host-status {enable disable }	Enable to route the email to a specific SMTP server or relay.	disable
bcc-addr <email_address>	Type the BCC recipient email addresses for sending a blind carbon copy (BCC) of the email.	No default.
bcc-status {enable disable }	Enable to send a blind carbon copy (BCC) of the email.	disable

Variable	Description	Default
header-insertion-name <name_str>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as infected by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-value <header_str>.</p>	
header-insertion-status {enable disable }	<p>Enable to add a message header to infected email.</p> <p>See header-insertion-value <header_str>.</p>	disable
header-insertion-value <header_str>	<p>Enter the message header value.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as infected by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-name <name_str>.</p>	
notification-profile <name_string>	Type the name of the notification profile used for sending notifications.	No default.
notification-status {enable disable }	Enable sending notifications using a notification profile.	disable
subject-tagging-status {enable disable }	Enable to prepend text ("tag") defined using subject-tagging-text <tag_str> to the subject line on infected email.	disable

Variable	Description	Default
subject-tagging-text <tag_str>	Enter the text that will appear in the subject line of the email, such as "[VIRUS]". The FortiMail unit will prepend this text to the subject line of the email before forwarding it to the recipient.	
rewrite-rcpt-local-type {none prefix replace suffix}	<p>Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any infected email message.</p> <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>. 	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none prefix replace suffix} .	
rewrite-rcpt-domain-type {none-prefix replace suffix}	<p>Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any infected email message.</p> <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. 	none
rewrite-rcpt-domain-value <value_str>	Type the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix replace suffix} .	

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile authentication

Use this sub-command to configure the FortiMail unit to connect to an external SMTP server in order to authenticate email users.

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS

When the FortiMail unit is operating in server mode, only local and RADIUS authentication are available.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine.

Depending on the mode in which your FortiMail unit is operating, you may be able to apply authentication profiles through inbound recipient-based policies, IP-based policies, and email user accounts.

For more information, see the *FortiMail Administration Guide*.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile authentication imap
    edit <profile_name>
        set option {ssl | secure | tls | senddomain}
        set port <port_int>
        set server {<fqdn_str> | <host_ipv4>}
config profile authentication pop3
    edit <profile_name>
        set option {ssl | secure | tls | senddomain}
        set port <port_int>
        set server {<fqdn_str> | <host_ipv4>}
config profile authentication radius
    edit <profile_name>
        set auth-prot {auto | chap | mschap | mschap2 | pap}
        set nas-ip <ip_addr>
        set port <port_int>
        set secret <password_str>
        set send-domain {enable | disable}
        set server {<fqdn_str> | <host_ipv4>}
config profile authentication smtp
    edit <profile_name>
        set option {ssl | secure | tls | senddomain}
        set server {<fqdn_str> | <host_ipv4>}
        set port <port_int>
        set try-ldap-mailhost {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
option {ssl secure tls senddomain}	Enter one or more of the following in a space-delimited list: <ul style="list-style-type: none"> senddomain: Enable if the IMAP server requires both the user name and the domain when authenticating. ssl: Enables secure socket layers (SSL) to secure message transmission. secure: Enables secure authentication. tls: Enables transport layer security (TLS) to ensure privacy between communicating application 	No default.
port <port_int>	Enter the TCP port number of the IMAP server. The standard port number for IMAP is 143; for SSL-secured IMAP, it is 993.	143
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the IMAP server.	No default.
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: <ul style="list-style-type: none"> domain: Enable if the POP3 server requires both the user name and the domain when authenticating. ssl: Enables secure socket layers (SSL) to secure message transmission. secure: Enables secure authentication. tls: Enables transport layer security (TLS) to ensure privacy between communicating application 	No default.
port <port_int>	Enter the TCP port number of the POP3 server. The standard port number for POP3 is 110; for SSL-secured POP3, it is 995.	110
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the POP3 server.	No default.
auth-prot {auto chap mschap mschap2 pap}	Enter the authentication method for the RADIUS server. This option is available in server mode only.	auto
nas-ip <ip_addr>	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiMail interface uses to communicate with the RADIUS server will be applied. This option is available in server mode only.	0.0.0.0
port <port_int>	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server. The standard port number for RADIUS is 1812.	1812

Variable	Description	Default
secret <password_str>	Enter the password for the RADIUS server.	No default.
send-domain {enable disable }	Enable if the RADIUS server requires both the user name and the domain when authenticating.	disable
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the RADIUS server.	No default.
option {ssl secure tls senddomain}	<p>If you want to enable any of the following options, enter them in a space-delimited list:</p> <ul style="list-style-type: none"> <code>senddomain</code>: Enable if the SMTP server requires both the user name and the domain when authenticating. <code>ssl</code>: Enables secure socket layers (SSL) to secure message transmission. <code>secure</code>: Enables secure authentication. <code>tls</code>: Enables transport layer security (TLS) to ensure privacy between communicating application 	No default.
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	No default.
port <port_int>	<p>Enter the TCP port number of the SMTP server.</p> <p>The standard port number for SMTP is 25; for SSL-secured SMTP, it is 465.</p>	25
try-ldap-mailhost {enable disable}	<p>Enable if your LDAP server has a mail host entry for the generic user</p> <p>If you select this option, the FortiMail unit will query the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will query the server you entered in the server field.</p>	enable

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile content

Use this sub-command to create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

Unlike antispam profiles, which deal primarily with spam, content profiles match any other type of email.

Content profiles can be used to apply content-based encryption to email. They can also be used to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. As such, content profiles can be used both for email that you want to protect, and for email that you want to prevent.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile content
  edit <profile_name>
    set action-default {predefined-content-basic | content-def}
    set action-encrypted {predefined-content-basic | content-def}
    set action-image {predefined-content-basic | content-def}
    set archive-block-on-failure-to-decompress {enable | disable}
    set archive-block-password-protected {enable | disable}
    set archive-block-recursive {enable | disable}
    set archive-content-check {enable | disable}
    set archive-max-recursive-level <threshold_int>
    set attachment-name-disposition {block | pass}
    set attachment-type-disposition {block | pass}
    set block-msg-fragmented {enable | disable}
    set block-msg-without-attachment {enable | disable}
    set bypass-on-auth {enable | disable}
    set defer-message-delivery {enable | disable}
    set defersize <threshold_int>
    set filetype-application-other {enable | disable}
    set filetype-archive {enable | disable}
    set filetype-audio {enable | disable}
    set filetype-document {enable | disable}
    set filetype-document-msoffice {enable | disable}
    set filetype-document-msoffice-embedded-check
      {enable | disable}
    set filetype-document-msoffice-vba-check {enable | disable}
    set filetype-document-openoffice {enable | disable}
    set filetype-document-openoffice-embedded-check
      {enable | disable}
    set filetype-document-other {enable | disable}
    set filetype-document-pdf {enable | disable}
    set filetype-document-visio {enable | disable}
    set filetype-document-visio-embedded-check {enable | disable}
    set filetype-encrypted {enable | disable}
    set filetype-encrypted-pgp {enable | disable}
    set filetype-encrypted-smime {enable | disable}
    set filetype-executable {enable | disable}
    set filetype-executable-activex {enable | disable}
    set filetype-executable-java {enable | disable}
    set filetype-executable-javascript {enable | disable}
    set filetype-executable-other {enable | disable}
    set filetype-executable-vba {enable | disable}
    set filetype-executable-vbs {enable | disable}
    set filetype-image {enable | disable}
    set filetype-image-gif {enable | disable}
    set filetype-image-jpeg {enable | disable}
    set filetype-image-other {enable | disable}
```

```

set filetype-image-png {enable | disable}
set filetype-image-tiff {enable | disable}
set filetype-text {enable | disable}
set filetype-text-7bit {enable | disable}
set filetype-text-html {enable | disable}
set filetype-text-other {enable | disable}
set filetype-text-xml {enable | disable}
set filetype-video {enable | disable}
set remove-hidden-html-content {enable | disable}
config attachment-name
    edit attachment-name-pattern <pattern_str>
        set status {enable | disable}
    next
end
config monitor
    edit monitor <index_int>
        set action <action-profile_name>
        set dict-score <score_int>
        set dictionary-group <dictionary-group_name>
        set dictionary-profile <dictionary-profile_name>
        set dictionary-type {group | profile}
        set scan-msoffice {enable | disable}
        set scan-pdf {enable | disable}
        set status {enable | disable}
    next
end
next
end

```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
action-default {predefined-content-basic content-def}	Enter a predefined content action profile for attachment filtering.	No default.
action-encrypted {predefined-content-basic content-def}	Enter a predefined content action profile for filtering email with encrypted content, such as PGP. Encrypted email content cannot be scanned for spam, viruses, or banned content.	No default.
action-image {predefined-content-basic content-def}	Enter a predefined content action profile for filtering email containing images, such as GIF.	No default.
archive-block-on-failure-to-decompress {enable disable }	Enter to apply the action configured in “ config profile content-action ” on page 125 if an attached archive cannot be successfully decompressed in order to scan its contents.	disable

Variable	Description	Default
archive-block-password-protected {enable disable}	Enter to apply the action configured in “ config profile content-action ” on page 125 if an attached archive is password-protected.	disable
archive-block-recursive {enable disable}	Enable to block archive attachments whose depth of nested archives exceeds archive-max-recursive-level <threshold_int> .	enabled
archive-content-check {enable disable}	Enter to enable consideration of the nesting depth threshold, password protection, and successful decompression when scanning attachments that are archives.	enabled
archive-max-recursive-level <threshold_int>	<p>Enter the nesting depth threshold. Depending upon each attached archive’s depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email.</p> <ul style="list-style-type: none"> • archive-max-recursive-level is 0, or attachment’s depth of nesting equals or is less than archive-max-recursive-level: If the attachment contains a file that matches one of the other MIME file types, perform the action configured for that file type, either block or pass. • Attachment’s depth of nesting is greater than archive-max-recursive-level: Apply the block action, unless you have disabled archive-block-recursive {enable disable}, in which case it will pass the MIME file type content filter. Block actions are specified in “profile content-action” on page 198. <p>This option applies only if archive-content-check {enable disable} is enabled.</p>	0
attachment-name-disposition {block pass}	<p>Pass or block email if a file attachment matches the file name patterns enabled in attachment-name-pattern <pattern_str>.</p> <p>If an attachment matches a pattern not enabled, the FortiMail unit will perform the opposite action of whatever you selected, either block or pass.</p> <p>For example, if you enter <code>block</code> and have enabled the name pattern <code>*.exe</code>, files whose names end in <code>.exe</code> will be blocked. All other file names will pass attachment filtering, but will still be subject to any other filters or antispam scans that you have configured.</p> <p>Conversely, if you select <code>pass</code> and enabled <code>*.doc</code>, all file names other than those ending in <code>.doc</code> will be blocked.</p>	block

Variable	Description	Default
attachment-type-disposition {block pass}	Block or pass email if a file attachment matches the file types enabled in <code>attachment-type <MIME-type_str></code> . File types that you have not enabled will receive the action opposite of your block/pass selection. Passed file types will pass attachment file type filtering only, and will still be subject to any other content filters or antispam scans that you have configured.	block
block-msg-fragmented {enable disable}	Enable to detect and block fragmented email. Some mail user agents, such as Outlook, can fragment big emails into multiple sub-messages. This is used to bypass oversize limits/scanning.	disable
block-msg-without-attachment {enable disable}	Enable to apply the block action configured in the content action profile if an email does not have any attachments.	disable
bypass-on-auth {enable disable}	Enable to omit antispam scans when an SMTP sender is authenticated.	disable
defer-message-delivery {enable disable}	Enable to defer mail delivery from specific senders configured in policy to conserve peak time bandwidth at the expense of sending low priority, bandwidth consuming traffic at scheduled times. For example, you can apply this function to senders of marketing campaign emails or mass mailing.	disable
defersize <threshold_int>	Enter the size threshold in kilobytes. Delivery of email messages greater than this size will be deferred until the period configured for oversize email. To disable deferred delivery, enter 0.	0
filetype-application-other {enable disable}	Enable to block all file types not specifically described by the other options.	disable
filetype-archive {enable disable}	Enable to block emails that contain archive content to pass the attachment file type filter.	disable
filetype-audio {enable disable}	Enable to block emails that contain audio content to pass the attachment file type filter.	disable
filetype-document {enable disable}	Enable to block emails that contain document content to pass the attachment file type filter.	disable
filetype-document-msoffice {enable disable}	Enable to block emails that contain Microsoft Office content to pass the attachment file type filter.	disable

Variable	Description	Default
filetype-document -msoffice-embedded-check {enable disable }	Enable to block emails that contain Microsoft Office content with embedded checking script to pass the attachment file type filter.	disable
filetype-document -msoffice-vba-check {enable disable }	Enable to block emails that contain Microsoft Office content with VBA checking script to pass the attachment file type filter.	disable
filetype-document -openoffice {enable disable }	Enable to block emails that contain OpenOffice content to pass the attachment file type filter.	disable
filetype-document -openoffice-embedded-check {enable disable }	Enable to block emails that contain OpenOffice content with embedded checking script to pass the attachment file type filter.	disable
filetype-document -other {enable disable }	Enable to block emails that contain all other document types not specifically described by the other options to pass the attachment file type filter.	disable
filetype-document -pdf {enable disable }	Enable to block emails that contain PDF content to pass the attachment file type filter.	disable
filetype-document -visio {enable disable }	Enable to block emails that contain Visio content with embedded checking script to pass the attachment file type filter.	disable
filetype-document -visio-embedded-check {enable disable }	Enable to block emails that contain Visio content with embedded checking script to pass the attachment file type filter.	disable
filetype-encrypted {enable disable }	Enable to block emails that contain encrypted content to pass the attachment file type filter.	disable
filetype-encrypted-pgp {enable disable }	Enable to block emails that contain encrypted PGP content to pass the attachment file type filter.	disable
filetype-encrypted-smime {enable disable }	Enable to block emails that contain encrypted SMIME content to pass the attachment file type filter.	disable

Variable	Description	Default
filetype-executable {enable disable }	Enable to block emails that contain executable content to pass the attachment file type filter.	disable
filetype-executable-activex {enable disable }	Enable to block emails that contain Activex executable content to pass the attachment file type filter.	disable
filetype-executable-java {enable disable }	Enable to block emails that contain Java executable content to pass the attachment file type filter.	disable
filetype-executable-javascript {enable disable }	Enable to block emails that contain Java Script executable content to pass the attachment file type filter.	disable
filetype-executable-other {enable disable }	Enable to block emails that contain all other executable content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-executable-vba {enable disable }	Enable to block emails that contain VBA executable content to pass the attachment file type filter.	disable
filetype-executable-vbs {enable disable }	Enable to block emails that contain VBS executable content to pass the attachment file type filter.	disable
filetype-image {enable disable }	Enable to block emails that contain image content to pass the attachment file type filter.	disable
filetype-image-gif {enable disable }	Enable to block emails that contain GIF image content to pass the attachment file type filter.	disable
filetype-image-jpeg {enable disable }	Enable to block emails that contain JPEG image content to pass the attachment file type filter.	disable
filetype-image-other {enable disable }	Enable to block emails that contain all other image content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-image-png {enable disable }	Enable to block emails that contain PNG image content to pass the attachment file type filter.	disable
filetype-image-tiff {enable disable }	Enable to block emails that contain TIFF image content to pass the attachment file type filter.	disable

Variable	Description	Default
filetype-text {enable disable }	Enable to block emails that contain text content to pass the attachment file type filter.	disable
filetype-text-7bit {enable disable }	Enable to block emails that contain 7bit text content to pass the attachment file type filter.	disable
filetype-text-html {enable disable }	Enable to block emails that contain HTML content to pass the attachment file type filter.	disable
filetype-text-other {enable disable }	Enable to block emails that contain all other text content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-text-xml {enable disable }	Enable to block emails that contain XML content to pass the attachment file type filter.	disable
filetype-video {enable disable }	Enable to block emails that contain video content to pass the attachment file type filter.	disable

Variable	Description	Default
remove-hidden-html-content {enable disable }	<p>Enable to detect hypertext markup language (HTML) tags and, if found:</p> <ul style="list-style-type: none"> • apply the content profile • add X-FEAS-ATTACHMENT-FILTER: Contains HTML tags. to the message headers <p>Use this option to mitigate potentially harmful HTML content such as corrupted images or files, or phishing URLs that are specially crafted for a targeted attack, and not yet identified by the FortiGuard Antispam service.</p> <p>Depending on the action profile, for example, you could warn email users by tagging email that contains potentially dangerous HTML content, or, if you have removed the HTML tags, allow users to safely read the email to decide whether or not it is legitimate first, without automatically displaying and executing potentially dangerous scripts, images, or other files. (Automatic display of HTML content is a risk on some email clients.)</p> <p>Caution: <i>Unless</i> you also select <i>Replace</i> in the content action profile, HTML is not removed, and the email will not be converted to plain text. Instead, the FortiMail unit will only apply whichever other action profile “block” action you have selected.</p> <p>To actually remove HTML tags, you must also select Replace.</p> <p>If you select <i>Replace</i>, all HTML tags are removed, except for the minimum required by the HTML document type definition (DTD): <html>, <head>, and <body>.</p> <p>Stripped body text is surrounded by <pre> tags, which is typically rendered in a monospace font, causing the appearance to mimic plain text.</p> <p>For linked files, which are hosted on an external web site for subsequent download rather than directly attached to the email, the FortiMail unit will download and attach the file to the email before removing the or <embed> tag. In this way, while the format is converted to plain text, attachments and linked files which may be relevant to the content are still preserved.</p> <p>For example, in an email is a mixture of HTML and plain text (Content-Type: multipart/alternative), and the action profile’s “block” action is <i>Replace</i>, the FortiMail unit removes hyperlink, font, and other HTML tags in the sections labeled with Content-Type: text/html. Linked images are converted to attachments. (The MIME Content-Type: text/html label itself is not be modified.)</p>	disable

Variable	Description	Default
attachment-name-pattern <pattern_str>	<p>Enter a pattern, such as ' *.bat ', that matches the email attachment names that you want the content profile to match.</p> <p>The patterns include:</p> <ul style="list-style-type: none"> • *.bat • *.com • *.dll • *.doc • *.exe • *.gz • *.hta • *.ppt • *.rar • *.scr • *.tar • *.tgz • *.vb? • *.wps • *.xl? • *.zip • *.pif 	No default.

Variable	Description	Default
attachment-type <MIME-type_str>	<ul style="list-style-type: none"> • Enter one of the following MIME types or subtypes: • video • audio • image • image-gif • image-jpeg • image-tiff • image-png • image-other: This option includes all images not specified by the other image types. • executable • executable-activex • executable-java • executable-javascript • executable-vbs • executable-vba • executable-other: This option includes all executables not specified by the other executable types. • document • document-msoffice • document-msoffice-embedded-check • document-msoffice-vba-check • document-visio • document-visio-vba-check • document-openoffice • document-openoffice-embedded-check • document-pdf • document-other: This option includes all documents not specified by the other document types. • archive • application-other: This option includes all applications not specified by the other application types. • text • text-7bit • text-html • text-xml • text-other: This option includes all text documents not specified by the other text types. • encrypted: This option includes both the S/MIME type and PGP-encrypted email. 	
status {enable disable }	Enable or disable a pattern that matches the email attachment names that you want the content profile to match.	disable

Variable	Description	Default
monitor <index_int>	Enter the index number of the monitor profile. If the monitor profile does not currently exist, it will be created.	No default.
action <action-profile_name>	Enter the action profile for this monitor profile. The FortiMail unit will perform the actions if the content of the email message matches words or patterns from the dictionary profile that the monitor profile uses.	No default.
dict-score <score_int>	Enter the number of times that an email must match the content monitor profile before it will receive the action configured in action <action-profile_name> .	1
dictionary-group <dictionary-group_name>	Enter the dictionary profile group that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profiles. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in action <action-profile_name> . This option is available only when dictionary-type {group profile} is <code>group</code> . For information on dictionary profiles, see the <i>FortiMail Administration Guide</i> .	No default.
dictionary-profile <dictionary-profile_name>	Enter the dictionary profile that this monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profile. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in action <action-profile_name> . For information on dictionary profiles, see the <i>FortiMail Administration Guide</i> .	No default.
dictionary-type {group profile}	Enter profile to detect content based upon a dictionary profile, or group to detect content based upon a group of dictionary profiles. Depending on your selection, also configure either dictionary-group <dictionary-group_name> or dictionary-profile <dictionary-profile_name> .	group
scan-msoffice {enable disable}	Enable to scan the content of Microsoft Word files such as Word and Excel.	disable
scan-pdf {enable disable}	Enable to scan the content of PDF files.	disable
status {enable disable}	Enable or disable this monitor profile.	disable

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content-action](#)
- [config user mail](#)
- [config user group](#)

config profile content-action

Use this sub-command to define content action profiles.

Content action profiles can be used to apply content-based encryption.

Alternatively, content action profiles can define one or more things that the FortiMail unit should do if the content profile determines that an email contains prohibited words or phrases, file names, or file types.

For example, you might have configured most content profiles to match prohibited content, and therefore to use a content action profile named `quar_profile` which quarantines email to the system quarantine for review.

However, you have decided that email that does not pass the dictionary scan named `financial_terms` is ***always*** prohibited, and should be rejected so that it does not require manual review. To do this, you would first configure a second action profile, named `rejection_profile`, which rejects email. You would then override `quar_profile` specifically for the dictionary-based content scan in each profile by selecting `rejection_profile` for content that matches `financial_terms`.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config profile content-action
  edit <profile_name>
    set action {discard | encryption | none | quarantine |
               quarantine-review | reject | replace | rewrite-rcpt |
               treat-as-spam}
    set alternate-host <name/ip_string>
    set alternate-host-status {enable | disable}
    set archive-account <name_string>
    set archive-status {enable | disable}
    set bcc-addr <email_address>
    set bcc-status {enable | disable}
    set encryption-profile <name_string>
    set header-insertion-name <name_str>
    set header-insertion-value <header_str>
    set notification-profile <name_string>
    set notification-status {enable | disable}
    set subject-tagging-text <tag_str>
    set tagging-type {insert-header | tag-subject}
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
  next
end
```

Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
action {discard encryption none quarantine quarantine-review reject replace rewrite-rcpt treat-as-spam}	Type an action for the profile. <ul style="list-style-type: none"> discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. encryption: Enable to apply an encryption profile, then select which encryption profile to use. Also configure encryption-profile <name_string>. none: Apply any configured header or subject line tags, if any. quarantine: Enter to redirect the email to the per-recipient quarantine. For more information, see the FortiMail Administration Guide. quarantine-review: Enter to redirect the email to the system quarantine. For more information, see the FortiMail Administration Guide. reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. replace: Enable to replace the email's contents with a replacement message. rewrite-rcpt: Enter to change the recipient address of any email that matches the content profile. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). If you enter this option, also configure rewrite-rcpt-local-type {none prefix replace suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix replace suffix}, and rewrite-rcpt-domain-value <value_str>. treat-as-spam: Apply the action selected in the antispam profile. 	none
alternate-host <name/ip_string>	Type the name or IP address of the SMTP server or relay where you want to route the email to. If you enable this setting, the FortiMail unit uses this destination for all email that matches the profile.	No default.
alternate-host-status {enable disable }	Enable to route the email to a specific SMTP server or relay.	disable
archive-account <name_string>	Enable to send the email to an archiving account. As long as this action is enabled, no matter if the email is delivered or rejected, it will still be archived.	No default.

Variable	Description	Default
archive-status {enable disable }	Enable to send the email to an archiving account.	disable
bcc-addr <email_address>	Type the BCC recipient email addresses for sending a blind carbon copy (BCC) of the email.	No default.
bcc-status {enable disable }	Enable to send a blind carbon copy (BCC) of the email.	disable
encryption-profile <name_string>	If you selected quarantine in action {discard encryption none quarantine quarantine-review reject replace rewrite-rcpt treat-as-spam} , enter the encryption profile to use.	No default.
header-insertion-name <name_str>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as prohibited by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-value <header_str>.</p>	
header-insertion-value <header_str>	<p>Enter the message header value.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as prohibited by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See header-insertion-name <name_str>.</p>	
notification-profile <name_string>	Type the name of the notification profile used for sending notifications.	No default.

Variable	Description	Default
notification-status {enable disable}	Enable sending notifications using a notification profile.	disable
subject-tagging-text <tag_str>	Enter the text that will appear in the subject line of the email, such as "[PROHIBITED-CONTENT]". The FortiMail unit will prepend this text to the subject line of the email before forwarding it to the recipient.	No default.
tagging-type {insert-header tag-subject}	Enter the type of tagging for this profile. Enter <code>insert-header</code> enables <code>header-insertion-name <name_str></code> and <code>header-insertion-value <header_str></code> . Enter <code>tag-subject</code> enables <code>subject-tagging-text <tag_str></code> .	No default.
rewrite-rcpt-local-type {none prefix replace suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any prohibited email message. <ul style="list-style-type: none"> <code>none</code>: No change. <code>prefix</code>: Enter to prepend the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. <code>suffix</code>: Enter to append the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. <code>replace</code>: Enter to substitute the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. 	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except <code>none</code>) you choose in <code>rewrite-rcpt-local-type {none prefix replace suffix}</code>	No default.
rewrite-rcpt-domain-type {none-prefix replace suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any prohibited email message. <ul style="list-style-type: none"> <code>none</code>: No change. <code>prefix</code>: Enter to prepend the part with new text. Also configure <code>rewrite-rcpt-domain-value <value_str></code>. <code>suffix</code>: Enter to append the part with new text. Also configure <code>rewrite-rcpt-domain-value <value_str></code>. <code>replace</code>: Enter to substitute the part with new text. Also configure <code>rewrite-rcpt-domain-value <value_str></code>. 	none
rewrite-rcpt-domain-value <value_str>	Type the text for the option (except <code>none</code>) you choose in <code>rewrite-rcpt-domain-type {none-prefix replace suffix}</code> .	

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)

- [config profile authentication](#)
- [config profile content](#)
- [config user mail](#)
- [config user group](#)

config profile resource

Use this sub-command to define content action profiles which configure miscellaneous aspects of local email user accounts, such as disk space quota.

This option is in server mode only.

Syntax

This sub-command is available from within the command [dlp scan-rules](#).

```
config profile resource
  edit <profile_name>
    set auto-delete-old-mail <integer>
    set auto-delete-trash-folder <integer>
    set quota <integer>
    set status {enable | disable}
    set webmail-access {enable | disable}
  next
end
```

Variable	Description	Default
<profile_name>	Type the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
auto-delete-old-mail <integer>	Enter the number of days after which the FortiMail unit will automatically delete email that is locally hosted. 0 means never deleting email.	0
auto-delete-trash-folder <integer>	Enter the number of days after which the FortiMail unit will automatically delete email in the trash folder. 0 means never deleting email.	14
quota <integer>	Enter the maximum amount of FortiMail webmail disk space that you will allow to be consumed, or enter 0 to allow unlimited use.	100
status {enable disable }	Enable to apply this profile.	disable
webmail-access {enable disable }	Enable to allow email users to access FortiMail webmail.	disable

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)

- config policy recipient
- config profile antispam
- config profile antispam-action
- config profile antivirus
- config profile authentication
- config profile content
- config profile content-action
- config user group

config user mail

Use this sub-command to configure email user accounts.

Syntax

This sub-command is available from within the command `dlp scan-rules`.

```
config user mail
  rename <old_username> to <new_username> (see the note below)
  edit <user_name>
    set type {local | ldap}
    set type local
    set displayname <name_str>
    set password <pwd_str>
    set type ldap
    set displayname <name_str>
    set ldap-profile <ldap_name>
  next
end
```

Variable	Description	Default
<old_username>	The user account name you want to rename.	
<new_username>	The new user account name you want to change to.	
<user_name>	Enter the user name of an email user, such as <code>user1</code> . This is also the local-part portion of the email user's primary email address.	No default.
type {local ldap}	Enter the type of email user account you want to add. See set type local and set type ldap .	ldap
displayname <name_str>	Enter the display name of the local email user, such as 'User One'.	No default.
password <pwd_str>	Enter the password of the local email user.	No default.
displayname <name_str>	Enter the display name of the LDAP email user, such as 'User One'.	No default.
ldap-profile <ldap_name>	Enter the name of an LDAP profile in which authentication queries are enabled.	No default.



If you rename an existing user account to a new user account name, all the user's preferences and mail data will be ported to the new user. However, due to the account name change, the new user will not be able to decrypt and read the encrypted email that is sent to the old user name before.

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)
- [config profile content](#)
- [config profile content-action](#)
- [config user group](#)

config user group

Use this sub-command to group related email user accounts.

Email user groups can simplify the creation of policies: when creating policies, you can select the name of an email user group, rather than entering each email user name individually.

Syntax

This sub-command is available from within the command [dlp scan-rules](#).

```
config user group
  edit <group_name>
    set member member <user_str>
  end
```

Variable	Description	Default
<group_name>	Type the name of the email user group.	No default.
member <user_str>	Type the email users that are members of this user group.	No default.

Related topics

- [dlp scan-rules](#)
- [config domain-setting](#)
- [config policy recipient](#)
- [config profile antispam](#)
- [config profile antispam-action](#)
- [config profile antivirus](#)
- [config profile authentication](#)

- [config profile content](#)
- [config profile content-action](#)
- [config user mail](#)

domain-association

Note: This command applies only if the FortiMail unit is operating in gateway mode or transparent mode.

Use this command to configure domain associations. Associated domains use the settings of the protected domains or subdomains with which they are associated.

Domain associations can be useful for saving time when you have multiple domains for which you would otherwise need to configure protected domains with identical settings.

For example, if you have one SMTP server handling email for ten domains, you could create ten separate protected domains, and configure each with identical settings. Alternatively, you could create one protected domain, listing the nine remaining domains as domain associations. The advantage of using the second method is that you do not have to repeatedly configure the same things when creating or modifying the protected domains, saving time and reducing chances for error. Changes to one protected domain automatically apply to all of its associated domains.

Exceptions to settings that associated domains will re-use include DKIM keys and signing settings. Domain keys are by nature tied to the exact protected domain only, and cannot be used for any other protected domain, including associated domains.

Alternatively, you can configure LDAP queries to automatically add domain associations. For details, see [“system mailserver” on page 291](#).

Syntax

```
config domain-association
    edit <domain-association_fqdn>
        set main-domain <protected-domain_name>
    next
end
```

Variable	Description	Default
<domain-association_fqdn>	Enter the fully qualified domain name (FQDN) of a mail domain that you want to use the same settings as the same protected domain	No default.
<protected-domain_name>	Enter the name of the protected domain. The associated domain will use the settings of this domain.	No default.

Related topics

- [system mailserver](#)

file filter

File filters are used in the attachment scan rules. File filters defines the email attachment file types and file extensions to be scanned.

Syntax

```
config file filter
  edit <filter_type>
    set description
    set extension
    set mime-type
  end
```

Variable	Description	Default
<filter_type>	Enter the file attachment executable type to filter by.	No default.
description	Enter the description of the attachment filter.	No default.
extension	Enter the file extension, such as .exe or .dll.	
mime-type	Enter the mime type such as image or png.	

file signature

If you already have the SHA-1 (Secure Hash Algorithm 1) hash values of some known virus-infected files, you can add these values as file signatures and then, in the antivirus profile, enable the actions against these files. Use this command to add or edit the file signatures.

Syntax

```
config file signature
  edit <signature_type>
    set comments
  end
```

Variable	Description	Default
<signature_type>	Enter the file signature ID.	No default.
comments	Enter the general comments for the file signature.	No default.

log setting remote

Use this command to configure storing log messages remotely, on a Syslog server or FortiAnalyzer unit.

Syntax

```
config log setting remote
edit <log-destination_index>
    set comma-separated-value {enable | disable}
    set encryption-log-status {enable | disable}
    set event-log-category {admin configuration ha | imap pop3 smtp
        system update webmail}
    set event-log-status {enable | disable}
    set facility {alert | audit | auth | authpriv | clock | cron |
        daemon | ftp | kern | local0 | local1 | local2 | local3 |
        local4 | local5 | local6 | local7 | lpr | mail | news |
        ntp}
    set history-log-status {enable | disable}
    set loglevel {alert | critical | debug | emergency | error |
        information | notification | warning}
    set port <port_int>
    set protocol {syslog | cftps}
    set server <log_ipv4>
    set spam-log-status {enable | disable}
    set status {enable | disable}
    set virus-log-status {enable | disable}
end
```

Variable	Description	Default
<log-destination_index>	Type an index number to identify which remote Syslog server or FortiAnalyzer unit you are configuring.	No default.
comma-separated-value {enable disable }	Enable CSV format if you want to send log messages in comma-separated value (CSV) format. Note: Do not enable this option if the log destination is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV format logs.	disable
encryption-log-status {enable disable }	Enable or disable IBE event logging to a remote Syslog server or FortiAnalyzer unit.	disable

Variable	Description	Default
event-log-category {admin configuration ha imap pop3 smtp system update webmail}	<p>Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space.</p> <ul style="list-style-type: none"> admin: Log all administrative events, such as logins, resets, and configuration updates. configuration: Enable to log configuration changes. ha: Log all high availability (HA) activity. imap: Log all IMAP events. pop3: Log all POP3 events. smtp: Log all SMTP relay or proxy events. system: Log all system-related events, such as rebooting the FortiMail unit. update: Log both successful and unsuccessful attempts to download FortiGuard updates. webmail: Log all FortiMail webmail events. 	No default.
event-log-status {enable disable }	Enable or disable event logging to a remote Syslog server or FortiAnalyzer unit.	disable
facility {alert audit auth authpriv clock cron daemon ftp kern local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp}	<p>Type the facility identifier that the FortiMail unit will use to identify itself when sending log messages to the first Syslog server.</p> <p>To easily identify log messages from the FortiWeb unit when they are stored on the Syslog server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.</p>	kern
history-log-status {enable disable }	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	disable
loglevel {alert critical debug emergency error information notification warning}	<p>Type one of the following severity levels:</p> <ul style="list-style-type: none"> alert critical debug emergency error information notification warning <p>This log destination will receive log messages greater than or equal to this severity level.</p>	information

Variable	Description	Default
port <port_int>	If the remote host is a FortiAnalyzer unit, type 514. If the remote host is a Syslog server, type the UDP port number on which the Syslog server listens for connections.	514
protocol {syslog cftps}	Enter the protocol used for remote logging.	syslog
server <log_ipv4>	Type the IP address of the Syslog server or FortiAnalyzer unit.	No default.
spam-log-status {enable disable}	Enable to log all antispam events.	disable
status {enable disable}	Enable to send log messages to a remote Syslog server or FortiAnalyzer unit.	disable
virus-log-status {enable disable}	Enable to log all antivirus events.	disable

Related topics

- [log setting local](#)
- [log alertemail recipient](#)
- [log alertemail setting](#)

log setting local

Use this command to configure storing log messages to the local hard disk.

Syntax

```
config log setting local
    set antispam-log-status {enable | disable}
    set antivirus-log-status {enable | disable}
    set disk-full {overwrite | nolog}
    set encryption-log-status {enable | disable}
    set event-log-category {admin configuration ha | imap pop3 smtp
        system update webmail}
    set event-log-status {enable | disable}
    set history-log-status {enable | disable}
    set loglevel {alert | critical | debug | emergency | error |
        information | notification | warning}
    set rotation-hour <hour_int>
    set rotation-size <file-size_int>
    set rotation-period <days_int>
    set status {enable | disable}
    set sysevent-log-category
    set system-event-log-status
end
```

Variable	Description	Default
antispam-log-status {enable disable}	Enable to log all antispam events.	enable
antivirus-log-status {enable disable}	Enable to log all antivirus events.	enable
disk-full {overwrite nolog}	Enter the action the FortiMail unit will perform when the local disk is full and a new log message is caused. <ul style="list-style-type: none"> • overwrite: Delete the oldest log file in order to free disk space, and store the new log message. • nolog: Discard the new log message. 	overwrite
encryption-log-status {enable disable}	Enable to log all IBE events.	enable
event-log-category {admin configuration ha imap pop3 smtp system update webmail}	Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space. <ul style="list-style-type: none"> • admin: Log all administrative events, such as logins, resets, and configuration updates. • configuration: Enable to log configuration changes. • ha: Log all high availability (HA) activity. • imap: Log all IMAP events. • pop3: Log all POP3 events. • smtp: Log all SMTP relay or proxy events. • system: Log all system-related events, such as rebooting the FortiMail unit. • update: Log both successful and unsuccessful attempts to download FortiGuard updates. • webmail: Log all FortiMail webmail events. 	No default.
event-log-status {enable disable}	Enable or disable event logging to the local hard disk.	enable
history-log-status {enable disable}	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	disable

Variable	Description	Default
loglevel {alert critical debug emergency error information notification warning}	<p>Type one of the following severity levels:</p> <ul style="list-style-type: none"> • alert • critical • debug • emergency • error • information • notification • warning <p>This log destination will receive log messages greater than or equal to this severity level.</p>	information
rotation-hour <hour_int>	Enter the hour of the day when the rotation should start.	0
rotation-size <file-size_int>	<p>Enter the maximum size of the current log file in megabytes (MB).</p> <p>When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started).</p> <p>Starting from 5.2.4 release, the maximum allowed size is 500 MB. Before that, it was 1,000 MB.</p>	20
rotation-period <days_int>	<p>Enter the maximum age of the current log file in days.</p> <p>When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started).</p>	10
status {enable disable }	Enable to send log types which are enabled to the local hard disk.	enable
sysevent-log-category	System event log categories	
system-event-log-status	Enable/disable system event log	disable

Related topics

- [log setting remote](#)
- [log alertemail recipient](#)
- [log alertemail setting](#)

log alertemail recipient

Use this command to add up to 3 email addresses that will receive alerts.

Before the FortiMail unit can send alert email messages, you must configure it with one or more recipients.

You must also configure which categories of events will cause the FortiMail unit to send alert email message. For more information, see [“log alertemail setting” on page 140](#).

Syntax

```
config log alertemail recipient
  edit <recipient_email>
  next
end
```

Variable	Description	Default
<recipient_email>	Type an email address that will receive alert email.	No default.

Example

The following example configures alert email to be sent to three email addresses.

```
config log alertemail recipient
  edit admin@example.com
  next
  edit support@example.com
  next
  edit helpdesk@example.com
  next
end
```

Related topics

- [log setting remote](#)
- [log setting local](#)
- [log alertemail setting](#)

log alertemail setting

Use this command to configure which events will cause the FortiMail unit to send an alert email message.

Before the FortiMail unit can send an alert email message, you must select the event or events that will cause it to send an alert.

You must also configure alert email message recipients. For more information, see [“log alertemail recipient” on page 139](#).

Syntax

```
config log alertemail setting
  set categories {archivefailure critical deferq dictionary diskfull
    ha incidents quotafull systemquarantine}
  set deferq-interval <interval_int>
  set deferq-trigger <trigger_int>
  set license-interval <integer>
end
```

Variable	Description	Default
categories {archivefailure critical deferq dictionary diskfull ha incidents quotafull systemquarantine}	Enter a list of one or more of the following event types that will cause alert email: <ul style="list-style-type: none"> archivefailure: Email archiving to the remote host has failed. critical: The FortiMail unit has detected a system error. deferq: The deferred mail queue has exceeded the number of messages during the interval specified in <code>deferq-interval <interval_int></code> and <code>deferq-trigger <trigger_int></code>. dictionary: The dictionary database is corrupt. diskfull: The FortiMail unit's hard disk is full. ha: A high availability (HA) event such as failover has occurred. incidents: The FortiMail unit has detected a virus. Separate each option with a space. quotafull: An email user account has reached its disk space quota. systemquarantine: The system quarantine has reached its disk space quota. 	critical
deferq-interval <interval_int>	Enter the interval in minutes between checks of deferred queue size. This can be any number greater than zero.	30
deferq-trigger <trigger_int>	Enter the size that the deferred email queue must reach to cause an alert email to be sent. The valid range is 1 to 99999.	10000
license-interval <integer>	Enter the number of days (1-100) the FortiGuard license is to expire. An alert email is sent on the expiry day.	30

Related topics

- [log setting remote](#)
- [log setting local](#)
- [log alertemail recipient](#)

mailsetting host-mapping

Use this command to configure local host name mapping for email routing.

Syntax

```
config mailsetting host-mapping
    edit <host_name>
        set name <name_string>
        set mapped-host <host_name_string>
    end
```

Variable	Description	Default
<host_name>	Enter the local host name.	
name <name_string>	Enter the name for host mapping.	
mapped-host <host_name_string>	Enter the IPaddress or host name of mapped host.	

Related topics

- [log setting remote](#)
- [log setting local](#)
- [log alertemail recipient](#)

mailsetting mail-scan-options

Use this command to configure how to scan the compressed files.

Syntax

```
config mailsetting mail-scan-options
    set decompress-max-level <level_1_to_16>
    set decompress-max-size <size_in_MB>
    set scan-timeout-action {tempfail | passthrough}
    set scan-timeout-value <time-in-seconds>
end
```

Variable	Description	Default
decompress-max-level <level_1_to_16>	Specify how many levels to decompress the archived files for antivirus and content scan. Valid range is from 1 to 16.	12
decompress-max-size <size_in_MB>	Specify the maximum file size to scan after the archived files are decompressed. This applies to every single file after decompression. Bigger files will not be scanned.	10
scan-timeout-action {tempfail passthrough}	When the email attachments are large and the email scanning has timed out, FortiMail can either send a temporary fail message to the sender or just let the message pass through without further scanning.	tempfail
scan-timeout-value <time-in-seconds>	Specify how long FortiMail should spend on scanning email contents. The valid range is between 270 and 900 seconds. When the specified timeout has been reached, FortiMail will take the action specified above.	285 (seconds)

Related topics

- [mailsetting relay-host-list](#)

- mailsetting storage central-quarantine
- mailsetting storage central-quarantine
- mailsetting systemquarantine

mailsetting preference

When you configure antispam, antivirus, and content action profiles, you may use the following actions:

- Deliver to alternate host
- Deliver to original host
- System quarantine
- Personal quarantine

For the above actions, you can choose to deliver or quarantine the original email or the modified email. For example, when the HTML content is converted to text, if you choose to deliver the unmodified copy, the HTML version will be delivered; if you choose to deliver the modified copy, the plain text version will be delivered.

Syntax

```
config mailsetting preference
    set deliver-to-alternate-host {modified_copy | unmodified_copy}
    set deliver-to-original-host {modified_copy | unmodified_copy}
    set enforce-delivery
    set personal-quarantine {modified_copy | unmodified_copy}
    set personal-quarantine-attachment-scan
    set system-quarantine {modified_copy | unmodified_copy}
end
```

Variable	Description	Default
deliver-to-alternate-host {modified_copy unmodified_copy}	Specify to use the modified email or the unmodified email.	modified_copy
deliver-to-original-host {modified_copy unmodified_copy}	Specify to use the modified email or the unmodified email.	modified_copy
enforce-delivery	Enforce delivery action if delivery to original/alternative host is enabled	disable
personal-quarantine {modified_copy unmodified_copy}	Specify to use the modified email or the unmodified email.	modified_copy
personal-quarantine-attachment-scan	Enable or disable attachment scan for personal quarantined spam messages.	disable
system-quarantine {modified_copy unmodified_copy}	Specify to use the modified email or the unmodified email.	modified_copy

mailsetting proxy-smtp

Use this command to configure using the outgoing proxy instead of the built-in MTA for outgoing SMTP connections.

Note: This command applies only if the FortiMail unit is operating in transparent mode.

Syntax

```
config mailsetting proxy-smtp
    set proxy-original {enable | disable}
end
```

Variable	Description	Default
proxy-original {enable disable}	<p>Enable to, for outgoing SMTP connections, use the outgoing proxy instead of the built-in MTA.</p> <p>This allows the client to send email using the SMTP server that they specify, rather than enforcing the use of the FortiMail unit's own built-in MTA. The outgoing proxy will refuse the connection if the client's specified destination SMTP server is not available. In addition, it will not queue email from the SMTP client, and if the client does not successfully complete the connection, the outgoing proxy will simply drop the connection, and will not retry.</p> <p>Disable to relay email using the built-in MTA to either the SMTP relay defined in "mailsetting relay-host-list" on page 145, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (RCPT TO:) domain. The email may not actually travel through the unprotected SMTP server, even though it was the relay originally specified by the SMTP client. For details, see the <i>FortiMail Administration Guide</i>.</p> <p>Caution: If this option is enabled, consider also enabling <code>session-prevent-open-relay {enable disable}</code>. Failure to do so could allow clients to use open relays.</p> <p>Note: If this option is disabled, and an SMTP client is configured to authenticate, you must configure and apply an authentication profile. Without the profile, authentication with the built-in MTA will fail. Also, the mail server must be explicitly configured to allow relay in this case.</p> <p>Note: If this option is enabled, you will not be able to use IP pools. For more information, see "profile ip-pool" on page 211.</p> <p>Note: For security reasons, this option does not apply if there is no session profile selected in the applicable IP-based policy. For more information on configuring IP policies, see "policy ip" on page 160.</p>	disable

Related topics

- [mailsetting relay-host-list](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting systemquarantine](#)
- [debug application smtpproxy](#)

mailsetting relay-host-list

Use this command to configure the FortiMail unit's built-in MTA's connection to an SMTP relay, if any, to which the FortiMail unit will relay outgoing email. You can configure up to 8 relays.

This is typically provided by your Internet service provider (ISP), but could be a mail relay on your internal network.

If the SMTP relay's domain name resolves to more than one IP address, for each SMTP session, the FortiMail unit will randomly select one of the IP addresses from the result of the DNS query, effectively load balancing between the SMTP relays.

If you do not configure a relay server, for outgoing email delivered by the built-in MTA, the FortiMail unit will instead query the DNS server for the MX record of the mail domain in the recipient's email address (RCPT TO:), and relay the email directly to that mail gateway. For details, see the [FortiMail Administration Guide](#).



This option will be ignored for email that matches an antispam or content profile where you have enabled `alternate-host {<relay_fqdn> | <relay_ipv4>}`.

Syntax

```
config mailsetting relay-host-list
edit <relay-host-name>
    set auth-password <password_str>
    set auth-status {enable | disable}
    set auth-type {auto | plain | login | digest-md5 | cram-md5}
    set auth-username <user_str>
    set server-name <relay_fqdn>
    set server-port <port_int>
    set smtps {enable | disable}
end
```

Variable	Description	Default
<relay-host-name>	Enter the host name or IP address of the relay server.	
auth-password <password_str>	If <code>auth-status {enable disable}</code> is enable, enter the password of the FortiMail unit's user account on the SMTP relay.	No default.

Variable	Description	Default
auth-status {enable disable}	Enable if the SMTP relay requires authentication using the SMTP AUTH command. Also configure <code>auth-username <user_str></code> , <code>auth-password <password_str></code> , and <code>auth-type {auto plain login digest-md5 cram-md5}</code> .	disable
auth-type {auto plain login digest-md5 cram-md5}	If <code>auth-status {enable disable}</code> is enable, enter either the SMTP authentication type required by the SMTP relay when the FortiMail unit sends the ESMTP AUTH command, or enter <code>auto</code> to automatically detect and use the most secure authentication type supported by the relay server.	auto
auth-username <user_str>	If <code>auth-status {enable disable}</code> is enable, enter the name of the FortiMail unit's user account on the SMTP relay.	No default.
server-name <relay_fqdn>	Enter the fully qualified domain name (FQDN) of the SMTP relay.	No default.
server-port <port_int>	Enter the TCP port number on which the SMTP relay listens.	25
smtps {enable disable}	Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiMail unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.	disable

Related topics

- [mailsetting proxy-smtp](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting systemquarantine](#)

mailsetting sender-email-addr-handling

Unqualified email address is a string without @ sign, such `abc`. If this feature is enabled, the Envelop sender (`MAIL FROM:`) will be rewritten to `abc@host.domain`, while the Header `From` and `Reply-to` will be rewritten to `abc@domain`. Host is the host name attribute of the FortiMail unit and domain is the local domain name attribute of the FortiMail unit.

Syntax

```
config mailsetting sender-email-addr-handling
    set rewrite-unqualified-sender-addr {enable | disable}
end
```

Variable	Description	Default
rewrite-unqualified-sender-addr {enable disable}	Enable or disable the unqualified email sender address rewriting feature.	disable

mailsetting smtp-rcpt-verification

Microsoft Office 365 does not accept a blank MAIL FROM:, which is the FortiMail default setting for SMTP recipient verification. Use this command to add an envelope from address to solve the problem.

Syntax

```
config mailsetting smtp-rcpt-verification
    set mail-from-addr <email_address>
end
```

Variable	Description	Default
mail-from-addr <email_address>	Specify the envelope MAIL FROM: address to use.	

mailsetting storage central-ibe

Use this command to configure storage of IBE encrypted email.

To reduce the storage resources required on lower-end FortiMail units, you can configure them to store encrypted email on a high-end FortiMail unit that you have configured to act as a centralized storage server.

Syntax

```
config mailsetting storage central-ibe
    set remote-storage-type {disable | from-client |
        to-server-over-ssl}
    set client-ip <client_ipv4>
    set server-name <name_str>
    set server-host <server_ipv4>
end
```

Variable	Description	Default
remote-storage-type {disable from-client to-server-over-ssl}	<p>Enter one of the following centralized IBE types:</p> <ul style="list-style-type: none"> disable: Centralized IBE storage is disabled. The FortiMail unit stores its IBE messages locally, on its own hard disks. from-client: Select this option to allow the FortiMail unit to act as a central IBE storage server and receive IBE email from the client FortiMail units. Also configure <code>client-ip <client_ip></code> for each FortiMail client. Note this feature is only available on the high-end FortiMail models (FortiMail 1000D and above). to-server-over-ssl: Select this option to allow the FortiMail unit to act as a central IBE storage client and send its IBE messages to the remote FortiMail server. Also configure <code>server-name <name_str></code> and <code>server-host <server_ip></code>. All FortiMail units can act as clients. 	disable
client-ip <client_ip>	<p>Enter the IP address of the FortiMail unit that is allowed to store its IBE email on this high-end FortiMail unit.</p> <p>For FortiMail 1000D, 2000A, 2000B, and VM04 models, you can enter a maximum of 10 IP addresses as clients. For FortiMail 3000C and above models, you can enter a maximum of 20 IP addresses.</p> <p>This variable applies only if <code>remote-storage-type</code> is <code>from-client</code>.</p>	No default.
server-name <name_str>	<p>Enter the name of the FortiMail unit that is acting as the central IBE storage server. This name may be the host name or any other name that uniquely identifies the central quarantine server.</p> <p>This variable applies only if <code>remote-storage-type</code> is <code>to-server-over-ssl</code>.</p>	No default.
server-host <server_ip>	<p>Enter the IP address of the FortiMail unit that is acting as the central IBE storage server.</p> <p>This variable applies only if <code>remote-storage-type</code> is <code>to-server-over-ssl</code>.</p>	No default.

mailsetting storage central-quarantine

Use this command to configure centralized storage of quarantined email. This command is only available on high-end models.

To reduce the storage resources required on lower-end FortiMail units, you can configure them to store quarantined email on a high-end FortiMail unit that you have configured to act as a centralized quarantine server.

Syntax

```
config mailsetting storage central-quarantine
  set remote-storage-type {disable | from-client | to-server-plain
    | to-server-over-ssl | unknow}
  set client-ip <client_ipv4>
  set server-name <name_str>
  set server-host <server_ipv4>
end
```

Variable	Description	Default
remote-storage-type {disable from-client to-server-plain to-server-over-ssl unknow}	<p>Enter one of the following centralized quarantine types:</p> <ul style="list-style-type: none"> disable: Centralized quarantine storage is disabled. The FortiMail unit stores its quarantines locally, on its own hard disks. from-client: Select this option to allow the FortiMail unit to act as a central quarantine server and receive quarantined messages from other client FortiMail units. Also configure <code>client-ip <client_ipv4></code> of the FortiMail clients. Note this feature is only available on the high-end FortiMail models (FortiMail 1000D and above). to-server-over-plain: Select this option to allow the FortiMail unit to act as a central quarantine client and send quarantined messages to the remote server in plain text. Also configure <code>server-name <name_str></code> and <code>server-host <server_ipv4></code> of the remote server. All FortiMail units can act as clients. to-server-over-ssl: Same as <code>to-server-plain</code>, except the connection uses SSL. unknown: Centralized quarantine storage is unknown. 	disable
client-ip <client_ipv4>	<p>Enter the IP address of the FortiMail unit that is allowed to store its quarantined email on this high-end FortiMail unit.</p> <p>For FortiMail 1000D, 2000A, 2000B, and VM04 models, you can enter a maximum of 10 IP addresses as clients. For FortiMail 3000C and above models, you can enter a maximum of 20 IP addresses.</p> <p>This variable applies only if <code>remote-storage-type</code> is <code>from-client</code>.</p>	No default.

Variable	Description	Default
server-name <name_str>	Enter the name of the FortiMail unit that is acting as the central quarantine server. This name may be the host name or any other name that uniquely identifies the central quarantine server. This variable applies only if remote-storage-type is to-server.	No default.
server-host <server_ipv4>	Enter the IP address of the FortiMail unit that is acting as the central quarantine server. This variable applies only if remote-storage-type is to-server.	No default.

Related topics

- [mailsetting proxy-smtp](#)
- [mailsetting relay-host-list](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting systemquarantine](#)
- [mailsetting storage central-quarantine](#)

mailsetting storage config

Use these commands to configure the FortiMail unit to store mail data such as queues and email user mailboxes either on its local hard disks, or on a network file storage (NFS or iSCSI) server.

If the FortiMail unit is operating in an HA group, remote storage may be required or recommended. For more information, see the [FortiMail Administration Guide](#).

Syntax

```
config mailsetting storage config
    set encryption-key
    set folder <folder_str>
    set host <host_str>
    set iscsi-id <id_str>
    set password <password_str>
    set port <port_int>
    set protocol {nfs | iscsi_server}
    set type {local | remote}
    set username <user-name_str>
end
```

Variable	Description	Default
encryption-key	Enter the key that will be used to encrypt data stored on the iSCSI server. Valid key lengths are between 6 and 64 single-byte characters. Applies only when <code>protocol</code> is <code>iscsi_server</code> .	
folder <folder_str>	Enter the directory path of the NFS export on the NAS server where the FortiMail unit will store email. Applies only when <code>protocol</code> is <code>nfs</code> .	
host <host_str>	Enter the IP address or fully qualified domain name (FQDN) of the NFS or iSCSI server.	
iscsi-id <id_str>	Enter the iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA). Applies only when <code>protocol</code> is <code>iscsi_server</code> .	
password <password_str>	Enter the password of the FortiMail unit's account on the iSCSI server. Applies only when <code>protocol</code> is <code>iscsi_server</code> .	
port <port_int>	Enter the TCP port number on which the NFS or iSCSI server listens for connections.	0
protocol {nfs iscsi_server}	Select the type of the NAS server: <code>nfs</code> : A network file system (NFS) server. If you select this option, enter the following information: <code>iscsi_server</code> : An Internet SCSI (Small Computer System Interface), also called iSCSI, server. If you select this option, enter the following information:	nfs
type {local remote}	Select whether to store email locally or on an NFS server.	local
username <user-name_str>	Enter the user name of the FortiMail unit's account on the iSCSI server. Applies only when <code>protocol</code> is <code>iscsi_server</code> .	

Related topics

- [mailsetting proxy-smtp](#)
- [mailsetting relay-host-list](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting systemquarantine](#)

mailsetting systemquarantine

Use this command to configure the system quarantine account settings.

For more information on the system quarantine administrator account, see the [FortiMail Administration Guide](#).

Syntax

```
config mailsetting systemquarantine
  set account <name_str>
  set password <password_str>
  set forward-address <recipient_str>
  set rotation-period <day_integer>
  set rotation-status {enable | disable}
end
```

Variable	Description	Default
account <name_str>	Enter the name for the system quarantine administrator account. Surround the account name with single quotes.	systemquarantine
password <password_str>	<p>Enter the password for the system quarantine administrator account. Surround the password with single quotes.</p> <p>The password may be entered either literally, or as a pre-encoded string prefixed with "Enc ". For example, you might enter either:</p> <ul style="list-style-type: none">• systemquarantine• 'Enc XXmkN/Q7euFe+yfBweeuLXgmv7SiSfsBsOZ6p ffiYZ4dQvrxxkKJvk5rNCiq7TwUEg7HUhCVGFO vyYNQ7MJhjk8ZCB94pIqdrjFv5ub/WMLDuF4Z 5'	forti12356net
forward-address <recipient_str>	Enter an email address to which all messages diverted to the system quarantine will be copied. Surround the email address with single quotes.	
rotation-period <day_integer>	Enter the period in days when the FortiMail unit rotates the current system quarantine folder ("Inbox"). When the folder reaches this period, the FortiMail unit renames the current folder based upon its creation date and rename date, and creates a new "Inbox" folder.	7
rotation-status {enable disable}	Enable or disable folder rotation.	enable

Related topics

- [mailsetting proxy-smtp](#)
- [mailsetting relay-host-list](#)
- [mailsetting storage central-quarantine](#)
- [mailsetting storage central-quarantine](#)

policy access-control receive

Use this command to configure access control rules that apply to SMTP sessions being **received** by the FortiMail unit.

Access control rules, sometimes also called the access control list or ACL, specify whether the FortiMail unit will process and relay/proxy, reject, or discard email messages for SMTP sessions that are initiated by SMTP clients.

When an SMTP client attempts to deliver email through the FortiMail unit, the FortiMail unit compares each access control rule to the commands used by the SMTP client during the SMTP session, such as the envelope's sender email address (`MAIL FROM:`), recipient email address (`RCPT TO:`), authentication (`AUTH`), and TLS (`STARTTLS`). Rules are evaluated for a match in the order of their list sequence, from top to bottom. If all the attributes of a rule match, the FortiMail unit applies the action selected in the matching rule to the SMTP session, and no subsequent access control rules are applied.

Only one access control rule is ever applied to any given SMTP session.

Note: If no access control rules are configured, or no matching access control rules exist, **and** if the SMTP client is not configured to authenticate, the FortiMail unit will perform the default action, which varies by whether or not the recipient email address in the envelope (`RCPT TO:`) is a member of a protected domain.

- For protected domains, the default action is *RELAY*.
- For **un**protected domains, the default action is *REJECT*.

Without any configured access control rules, the FortiMail unit's access control prevents SMTP clients from using your protected server or FortiMail unit as an open relay: senders can deliver email incoming to protected domains, but cannot deliver email outgoing to unprotected domains.

If you want to allow SMTP clients such as your email users or email servers to send email to unprotected domains, you must configure at least one access control rule.

You may need to configure additional access control rules if, for example, you want to:

- discard or reject email from or to some email addresses, such as email addresses that no longer exist in your protected domain
- discard or reject email from some SMTP clients, such as a spammer that is not yet known to blacklists

Like IP-based policies, access control rules can reject connections based upon IP address.

Unlike IP-based policies, however, access control rules **cannot** affect email in ways that occur after the session's `DATA` command, such as by applying antispam profiles. Access control rules also cannot be overruled by recipient-based policies, and cannot match connections based upon the IP address of the SMTP server. (By the nature of how the ACL controls access to or through the FortiMail unit, the SMTP server is always the FortiMail unit itself, **unless** the FortiMail unit is operating in transparent mode.) For more information on IP-based policies, see the [FortiMail Administration Guide](#).

Syntax

```
config policy access-control receive
  edit <rule_id>
    set action {bypass | discard | reject | relay}
    set authenticated {any | authenticated | not-authenticated}
    set comment <string>
    set recipient-pattern <pattern_str>
    set recipient-pattern-type {default | group | regexp}
    set recipient-pattern-regexp {yes | no}
    set recipient-pattern-group <group_name>
    set reverse-dns-pattern <pattern_str>
    set reverse-dns-pattern-regexp {yes | no}
    set sender-ip-group <ip_group_name>
    set sender-ip-mask <ip&netmask_str>
    set sender-ip-type {ip-group | ip-mask}
    set sender-pattern <pattern_str>
    set sender-pattern-type {default | group | regexp}
    set sender-pattern-group <group_name>
    set sender-pattern-regexp {yes | no}
    set status {enable | disable}
    set tls-profile <profile_str>
  end
```

Variable	Description	Default
<rule_id>	Enter the number identifying the rule.	
action {bypass discard reject relay}	<p>Enter the action the FortiMail unit will perform for SMTP sessions matching this access control rule.</p> <ul style="list-style-type: none">• bypass: Relay or proxy and deliver the email, <i>but</i>, if the sender or recipient belongs to a protected domain, bypass all antispam profile processing. Antivirus, content and other scans will still occur.• discard: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client.• reject: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (Relaying denied).• relay: Relay or proxy, process, and deliver the email normally if it passes all configured scans.	relay

Variable	Description	Default
authenticated {any authenticated not-authenticated }	Enter a value to indicate whether this rule applies only to messages delivered by clients that have authenticated with the FortiMail unit. <ul style="list-style-type: none"> any: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit. authenticated: Match this access control rule only for clients that have authenticated with the FortiMail unit. not-authenticated: Match this access control rule only for clients that have not authenticated with the FortiMail unit. 	authenti_ cated
comment <string>	Enter any comments for access control rules for receiving email.	
recipient-pattern <pattern_str>	Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as \'*\').	*
recipient-pattern -type {default group regexp}	Enter the pattern type. <ul style="list-style-type: none"> default: This is the user defined pattern. Also configure <code>recipient-pattern <pattern_str></code>. group: If you enter this option, configure <code>recipient-pattern-group <group_name></code>. regexp: If you enter this option, configure <code>recipient-pattern-regexp {yes no}</code>. 	default
recipient-pattern -regexp {yes no}	Enter yes to use regular expression syntax instead of wildcards to specify the recipient pattern. This option is available only when <code>recipient-pattern-type {default group regexp}</code> is <code>regexp</code> .	no
recipient-pattern -group <group_name>	Enter the group name to specify the recipient pattern. This option is available only when <code>recipient-pattern-type {default group regexp}</code> is <code>group</code>	

Variable	Description	Default
reverse-dns-pattern <pattern_str>	<p>Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message.</p> <p>Because domain names in the SMTP session are self-reported by the connecting SMTP server and easy to fake, the FortiMail unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail does a DNS lookup using the SMTP server's IP address. The resulting domain name is compared to the reverse DNS pattern for a match. If the reverse DNS query fails, the access control rule match will also fail. If no other access control rule matches, the connection will be rejected with SMTP reply code 550 (Relaying denied).</p> <p>Wildcard characters allow you to enter partial patterns that can match multiple reverse DNS lookup results. An asterisk (*) represents one or more characters; a question mark (?) represents any single character.</p> <p>For example, the recipient pattern <code>mail*.com</code> will match messages delivered by an SMTP server whose domain name starts with "mail" and ends with ".com".</p> <p>Note: Reverse DNS queries for access control rules require that the domain name be a valid top level domain (TLD). For example, ".lab" is not a valid top level domain name, and thus the FortiMail unit cannot successfully perform a reverse DNS query for it.</p>	*
reverse-dns-pattern-regex {yes no}	Enter <code>yes</code> to use regular expression syntax instead of wildcards to specify the reverse DNS pattern.	no
sender-ip-group <ip_group_name>	<p>Enter the IP group of the SMTP client attempting to deliver the email message.</p> <p>This option only appears if you enter <code>ip-group</code> in <code>sender-ip-type {ip-group ip-mask}</code>.</p>	
sender-ip-mask <ip&netmask_str>	<p>Enter the IP address and netmask of the SMTP client attempting to deliver the email message. Use the netmask, the portion after the slash (/), to specify the matching subnet.</p> <p>For example, enter <code>10.10.10.10/24</code> to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as <code>10.10.10.0/24</code> in the access control rule table, with the 0 indicating that any value is matched in that position of the address.</p> <p>Similarly, <code>10.10.10.10/32</code> will appear as <code>10.10.10.10/32</code> and match only the 10.10.10.10 address.</p> <p>To match any address, enter <code>0.0.0.0/0</code>.</p>	0.0.0.0 0.0.0.0

Variable	Description	Default
sender-ip-type {ip-group ip-mask}	Select the method of the SMTP client attempting to deliver the email message. Also configure <code>sender-ip-mask <ip&netmask_str></code> and <code>sender-ip-group <ip_group_name></code> .	ip-mask
sender-pattern <pattern_str>	Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as <code>'*'</code>). This option is only available if you enter <code>default</code> in <code>sender-pattern-type {default group regexp}</code> .	*
sender-pattern-type {default group regexp}	Enter the pattern type. <ul style="list-style-type: none">• <code>default</code>: This is the user defined pattern. Also configure <code>sender-pattern <pattern_str></code>.• <code>group</code>: If you enter this option, configure <code>sender-pattern-group <group_name></code>.• <code>regexp</code>: If you enter this option, configure <code>sender-pattern-regexp {yes no}</code>.	default
sender-pattern-group <group_name>	Enter the group name to match any email address in the group. This option is only available if you enter <code>group</code> in <code>sender-pattern-type {default group regexp}</code> .	
sender-pattern-regexp {yes no}	Enter <code>yes</code> to use regular expression syntax instead of wildcards to specify the sender pattern. This option is only available if you enter <code>regexp</code> in <code>sender-pattern-type {default group regexp}</code> .	no
status {enable disable }	Enter <code>enable</code> to activate this rule.	enable
tls-profile <profile_str>	Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile. <ul style="list-style-type: none">• If the attributes match, the access control action is executed.• If the attributes do not match, the FortiMail unit performs the <i>Failure</i> action configured in the TLS profile. For more information on TLS profiles, see the FortiMail Administration Guide .	

Related topics

- [policy access-control delivery](#)
- [policy ip](#)
- [policy recipient](#)

policy access-control delivery

Use this command to configure delivery rules that apply to SMTP sessions being *initiated* by the FortiMail unit in order to deliver email.

Delivery rules enable you to require TLS for the SMTP sessions the FortiMail unit initiates when sending email to other email servers. They also enable you to apply identity-based encryption (IBE) in the form of secure MIME (S/MIME).

When initiating an SMTP session, the FortiMail unit compares each delivery rule to the domain name portion of the envelope recipient address (RCPT TO:), and to the IP address of the SMTP server receiving the connection. Rules are evaluated for a match in the order of their list sequence, from top to bottom. If a matching delivery rule does not exist, the email message is delivered. If a match is found, the FortiMail unit compares the TLS profile settings to the connection attributes and the email message is sent or the connection is not allowed, depending on the result; if an encryption profile is selected, its settings are applied. No subsequent delivery rules are applied. Only one delivery rule is ever applied to any given SMTP session.

Syntax

```
config policy access-control delivery
  edit <rule_id>
    set comment <string>
    set destination <ip&netmask_str>
    set encryption-profile <profile_str>
    set recipient-pattern <pattern_str>
    set sender-pattern <pattern_str>
    set status {enable | disable}
    set tls-profile <profile_str>
  end
```

Variable	Description	Default
<rule_id>	Enter the number identifying the rule.	
comment <string>	Enter any comments for email delivery rules.	
destination <ip&netmask_str>	<p>Enter the IP address and netmask of the system to which the FortiMail unit is sending the email message. Use the netmask, the portion after the slash (/) to specify the matching subnet.</p> <p>For example, enter 10.10.10.10/24 to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as 10.10.10.0/24 in the access control rule table, with the 0 indicating that any value is matched in that position of the address.</p> <p>Similarly, 10.10.10.10/32 will appear as 10.10.10.10/32 and match only the 10.10.10.10 address.</p> <p>To match any address, enter 0.0.0.0/0.</p>	0.0.0.0 0.0.0.0

Variable	Description	Default
encryption-profile <profile_str>	<p>Enter an encryption profile to apply identity-based encryption, if a corresponding sender identity exists in the certificate bindings.</p> <p>For more information on encryption profiles, see the FortiMail Administration Guide.</p>	
recipient-pattern <pattern_str>	<p>Enter a complete or partial envelope recipient (RCPT TO:) email address to match.</p> <p>Wild card characters allow you to enter partial patterns that can match multiple recipient email addresses. The asterisk (*) represents one or more characters and the question mark (?) represents any single character.</p> <p>For example, the recipient pattern *@example.??? will match messages sent to any email user at example.com, example.net, example.org, or any other "example" domain ending with a three-letter top-level domain name.</p>	
recipient-pattern-type		
sender-pattern <pattern_str>	<p>Enter a complete or partial envelope sender (MAIL FROM:) email address to match.</p> <p>Wild card characters allow you to enter partial patterns that can match multiple sender email addresses. The asterisk (*) represents one or more characters and the question mark (?) represents any single character.</p> <p>For example, the sender pattern ??@*.com will match messages sent by any email user with a two letter email user name from any ".com" domain name.</p>	
sender-pattern-type		
status {enable disable }	Enter <code>enable</code> to activate this rule.	disable
tls-profile <profile_str>	<p>Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile.</p> <ul style="list-style-type: none"> If the attributes match, the access control action is executed. If the attributes do not match, the FortiMail unit performs the <i>Failure</i> action configured in the TLS profile. <p>For more information on TLS profiles, see the FortiMail Administration Guide.</p>	

Related topics

- [policy access-control receive](#)

- policy ip
- policy recipient

policy ip

Use this command to create policies that apply profiles to SMTP connections based upon the IP addresses of SMTP clients and/or servers.

Syntax

```
config policy ip
  edit <policy_int>
    set action {proxy-bypass | reject | scan | temp-fail}
    set client-ip-group <group_name>
    set client <client_ipv4mask>
    set client-type {ip-address | ip-group | ip-pool}
    set comment
    set exclusive {enable | disable}
    set profile-antispam <antispam-profile_name>
    set profile-antivirus <antivirus-profile_name>
    set profile-auth-type {imap | ldap | none | pop3 | radius |
      smtp}
    set profile-content <content-profile_name>
    set profile-dlp
    set profile-ip-pool <ip-pool_name>
    set profile-session <session-profile_name>
    set server-ip-group <group_name>
    set server <smtp-server_ipv4mask>
    set server-ip-pool <ip-pool_str>
    set server-type {ip-address | ip-group | ip-pool}
    set smtp-diff-identity {enable | disable}
    set smtp-diff-identity-ldap
    set smtp-diff-identity-ldap-profile
    set status {enable | disable}
    set use-for-smtp-auth {enable | disable}
  end
```


Variable	Description	Default
<policy_int>	Enter the index number of the IP-based policy.	
action {proxy-bypass reject scan temp-fail}	Enter an action for this policy: <ul style="list-style-type: none"> Proxy-bypass: Bypass the FortiMail unit's scanning. scan: Accept the connection and perform any scans configured in the profiles selected in this policy. reject: Reject the email and respond to the SMTP client with SMTP reply code 550, indicating a permanent failure. Fail Temporarily: Reject the email and indicate a temporary failure. 	scan
client-ip-group <group_name>	Enter the IP group of the SMTP client to whose connections this policy will apply. This option only appears if you enter ip-group in client-type {ip-address ip-group ip-pool}.	
client <client_ipv4mask>	Enter the IP address and subnet mask of the SMTP client to whose connections this policy will apply. To match all clients, enter 0.0.0.0/0.	192.168.224.1 5 255.255.255.2 55
client-type {ip-address ip-group ip-pool}	Enter the client type.	ip-address
comment	Enter a brief comment for the IP policy	
exclusive {enable disable }	Enable to omit evaluation of matches with recipient-based policies, causing the FortiMail unit to disregard applicable recipient-based policies and apply only the IP-based policy. Disable to apply any matching recipient-based policy in addition to the IP-based policy. Any profiles selected in the recipient-based policy will override those selected in the IP-based policy.	disable
profile-antispam <antispam-profile_name>	Enter the name of an outgoing antispam profile, if any, that this policy will apply.	
profile-antivirus <antivirus-profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-type {imap ldap none pop3 radius smtp}	Enter the type of the authentication profile that this policy will apply. The command profile-auth-<auth_type> appears for the type chosen. Enter the name of an authentication profile for the type.	

Variable	Description	Default
profile-content <content-profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	
profile-dlp	Enter the name of the dlop profile for this policy.	
profile-ip-pool <ip-pool_name>	Enter the name of the IP pool profile that you want to apply to connections matching the policy.	
profile-session <session-profile_name>	Enter the name of the session profile that you want to apply to connections matching the policy.	
server-ip-group <group_name>	Enter the name of the IP group profile that you want to apply to connections matching the policy. This option is only available when the <code>server-type</code> is <code>ip-group</code> .	
server <smtp-server_ipv4mask>	Enter the IP address and subnet mask of the SMTP server to whose connections this policy will apply. To match all servers, enter <code>0.0.0.0/0</code> . This option applies only for FortiMail units operating in transparent mode. For other modes, the FortiMail unit receives the SMTP connection, and therefore acts as the server.	0.0.0.0 0.0.0.0
server-ip-pool <ip-pool_str>	Enter the name of the ip pool to whose connections this policy will apply. This option is only available when the <code>server-type</code> is <code>ip-pool</code> .	
server-type {ip-address ip-group ip-pool}	Enter the SMTP server type o whose connections this policy will apply. Also configure <code>server <smtp-server_ipv4mask></code> , <code>server-ip-group <group_name></code> , and <code>server-ip-pool <ip-pool_str></code> .	ip-address
smtp-diff-identity {enable disable }	Enable to allow the SMTP client to send email using a different sender email address (MAIL FROM:) than the user name that they used to authenticate. Disable to require that the sender email address in the SMTP envelope match the authenticated user name.	disable
smtp-diff-identity-ldap	Verify smtp sender identity with LDAP for authenticated email.	disable
smtp-diff-identity-ldap-profile	ldap profile for smtp sender identity verification.	disable
status {enable disable }	Enable to apply this policy.	enable
use-for-smtp-auth {enable disable }	Enable to authenticate SMTP connections using the authentication profile configured in <code>profile-auth-type {imap ldap none pop3 radius smtp}</code> .	disable

Related topics

- [policy access-control receive](#)

- policy access-control delivery
- policy recipient

policy recipient

Use this command to create recipient-based policies based on the inbound or outbound directionality of an email message with respect to the protected domain.

Syntax

```
config policy recipient
  edit <policy_int>
    set auth-access-options {pop3 | smtp-auth | smtp-diff-identity |
      web}
    set certificate-required {yes | no}
    set pkiauth {enable | disable}
    set pkuser <user_str>
    set profile-antispam <antispam-profile_name>
    set profile-antivirus <antivirus-profile_name>
    set profile-auth-type {imap | ldap | none | pop3 | radius |
      smtp}
    set profile-content <content-profile_name>
    set profile-ldap <profile_name>
    set recipient-domain <domain_str>
    set recipient-name <local-part_str>
    set recipient-type {ldap-group | local group| user}
    set sender-domain <domain_str>
    set sender-name <local-part_str>
    set sender-type {ldap-group | local group| user}
    set smtp-diff-identity {enable | disable}
    set status {enable | disable}
  end
```

Variable	Description	Default
<policy_int>	Enter the index number of the recipient-based policy.	
auth-access-options {pop3 smtp-auth smtp-diff-identity web}	<p>Enter the method that email users matching this policy use to retrieve the contents of their per-recipient spam quarantine.</p> <ul style="list-style-type: none"> • pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine. • smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. • smtp-diff-identity: Allow email when the SMTP client authenticates with a different user name than the one that appears in the envelope's sender email address. You must also enter smtp-auth for this option to have any effect. • web: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine. <p>Note: Entering this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication.</p>	
certificate-required {yes no}	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter yes .	no
pkiauth {enable disable}	Enable if you want to allow email users to log in to their per-recipient spam quarantine by presenting a certificate rather than a user name and password.	disable
pkiuser <user_str>	If pkiauth is enable , enter the name of a PKI user, such as 'user1'. For information on configuring PKI users, see "user pki" on page 313.	
profile-antispam <antispam-profile_name>	Enter the name of an antispam profile, if any, that this policy will apply.	
profile-antivirus <antivirus-profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-type {imap ldap none pop3 radius smtp}	<p>Enter the type of the authentication profile that this policy will apply.</p> <p>The command profile-auth-<auth_type> appears for the type chosen. Enter the name of an authentication profile for the type.</p>	none
profile-content <content-profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	

Variable	Description	Default
<code>ldap_profile</code> <ldap-profile_name>	If recipient-type or sender-type is ldap-group, enter the name of an LDAP profile in which the group owner query has been enabled and configured.	
<code>recipient-domain</code> <domain_str>	Enter the domain part of recipient email address to define recipient (RCPT TO:) email addresses that match this policy.	
<code>recipient-name</code> <local-part_str>	Enter the local part of recipient email address to define recipient (RCPT TO:) email addresses that match this policy.	
<code>recipient-type</code> {ldap-group local group user}	Enter one of the following ways to define recipient (RCPT TO:) email addresses that match this policy. If you enter ldap-group, also configure profile-ldap by entering an LDAP profile in which you have enabled and configured a group query.	user
<code>sender-domain</code> <domain_str>	Enter the domain part of sender email address to define sender (MAIL FROM:) email addresses that match this policy.	
<code>sender-name</code> <local-part_str>	Enter the local part of sender email address to define sender (MAIL FROM:) email addresses that match this policy.	
<code>sender-type</code> {ldap-group local group user}	Enter one of the following ways to define sender (MAIL FROM:) email addresses that match this policy. If you enter ldap-group, also configure profile-ldap by entering an LDAP profile in which you have enabled and configured a group query.	user
<code>smtp-diff-identity</code> {enable disable}	Enable to allow the SMTP client to send email using a different sender email address (MAIL FROM:) than the user name that they used to authenticate. Disable to require that the sender email address in the SMTP envelope match the authenticated user name. This option is applicable only if smtp auth is used.	enable
<code>status</code> {enable disable}	Enable to apply this policy.	enable

Related topics

- [policy access-control receive](#)
- [policy access-control delivery](#)
- [policy ip](#)

profile antispam

Use this command to configure system-wide antispam profiles. To configure a domain-wide antispam profile, use [“config profile antispam” on page 99](#).

FortiMail units can use various methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, Bayesian scanning, and heuristic scanning. Antispam profiles contain settings for these features that you may want to vary by policy. Depending on the feature, before you configure antispam policies, you may need to enable the feature or configure its system-wide settings.

Syntax

```
config profile antispam
  edit <profile_name>
    config bannedwords
      edit <word_str>
        set subject {enable | disable}
        set body {enable | disable}
    config dnsbl-server
      edit <server_name>
    config surbl-server
      edit <server_name>
    config whitelistwords
      edit <word_str>
        set subject {enable | disable}
```

```

    set body {enable | disable}
set action-banned-word <action_profile>
set action-bayesian <action_profile_name>
set action-behavior-analysis <action_profile_name>
set action-deep-header <action_profile_name>
set action-default <action_profile_name>
set action-dictionary <action_profile_name>
set action-fortiguard <action_profile_name>
set action-fortiguard-blackip <action_profile_name>
set action-fortiguard-phishing-uri <action_profile_name>
set action-grey-list <action_profile_name>
set action-heuristic <action_profile_name>
set action-image-spam <action_profile_name>
set action-newsletter <action_profile_name>
set action-rbl <action_profile_name>
set action-spf-checking <action_profile_name>
set action-surbl <action_profile_name>
set action-suspicious-newsletter <action_profile_name>
set action-uri-filter <action_profile_name>
set action-virus <action_profile_name>
set aggressive {enable | disable}
set apply-action-default {enable | disable}
set banned-word {enable | disable}
set bayesian {enable | disable}
set behavior-analysis {enable | disable}
set bayesian-autotraining {enable | disable}
set bayesian-user-db {enable | disable}
set bayesian-usertraining {enable | disable}
set deepheader {enable | disable}
set deepheader-analysis {enable | disable}
set deepheader-check-ip {enable | disable}
set dict-score <score_int>
set dictionary {enable | disable}
set dnsbl {enable | disable}
set fortiguard-antispam {enable | disable}
set fortiguard-check-ip {enable | disable}
set fortiguard-phishing-uri {enable | disable}
set greylist {enable | disable}
set heuristic {enable | disable}
set heuristic-lower <threshold_int>
set heuristic-rules-percent <percentage_int>
set heuristic-upper {threshold_int}
set image-spam {enable | disable}
set scan-bypass-on-auth {enable | disable}
set scan-max-size <bytes_int>
set scan-pdf {enable | disable}
set spam-outbreak-protection {enable | disable}
set spf-checking {enable | disable}
set surbl {enable | disable}

```

```

set suspicious-newsletter-status {enable | disable}
set uri filter {enable | disable}
set uri-filter-status {enable | disable}
set whitelist-enable {enable | disable}
set whitelist-word {enable | disable}
end

```

Variable	Description	Default
<profile_name>	Enter the name of an antispam profile.	
<word_str>	Enter the banned word. You can use wildcards in banned words. But regular expressions are not supported. For more information about wildcards and regular expressions, see FortiMail Administration Guide.	
subject {enable disable }	Enable to check the subject line for the banned word.	disable
body {enable disable }	Enable to check the message body for the banned word.	disable
<server_name>	Enter a DNSBL server name to perform a DNSBL scan. The FortiMail unit will query DNS blacklist servers.	
<server_name>	Enter a SURBL server name to perform a SURBL scan. The FortiMail unit will query SURBL servers.	
<word_str>	Enter the whitelisted word to configure.	
subject {enable disable }	Enable to check the subject line for the whitelisted word.	disable
body {enable disable }	Enable to check the message body for the whitelisted word.	disable
action-banned-word <action_profile>	Enter the action profile that you want the FortiMail unit to use if the banned word scan determines that the email is spam.	
action-bayesian <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the Bayesian scan determines that the email is spam.	
action-behavior-analysis <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the behavior analysis scan determines that the email is spam.	
action-deep-header <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the deep header scan determines that the email is spam.	
action-default <action-profile_name>	Enter the default action profile that you want all scanners of the FortiMail unit to use. However, if you choose an action profile other than "default" for a scanner, this scanner will use the chose profile.	

Variable	Description	Default
action-dictionary <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam.	
action-fortiguard <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the FortiGuard Antispam scan determines that the email is spam.	
action-fortiguard-blackip <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the FortiGuard black IP scan determines that the email is spam.	
action-fortiguard-phishing-uri <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the FortiGuard phishing URI scan determines that the email is spam.	
action-grey-list <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the grey list scan determines that the email is spam.	
action-heuristic <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam.	
action-image-spam <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the image scan determines that the email is spam.	
action-newsletter <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the newsletter scan determines that the email is spam.	
action-rbl <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the RBL scan determines that the email is spam.	
action-spf-checking <action-profile_name>	Enter the action profile you want the FortiMail unit to use if the SPF scan determines that the email is spam.	
action-surbl <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the SURBL scan determines that the email is spam.	
action-suspicious-newsletter <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the suspicious newsletter scan determines that the email is spam.	
action-uri-filter <action-profile_name>	Enter the action profile that you want the FortiMail unit to use if the URI filter scan determines that the email is spam.	
action-virus <action-profile_name>	Enter the action profile that requires the FortiMail unit to treat messages with viruses as spam.	
aggressive {enable disable }	<p>Enable this option to examine file attachments in addition to embedded images.</p> <p>To improve performance, enable this option only if you do not have a satisfactory spam detection rate.</p>	disable

Variable	Description	Default
apply-action-default {enable disable }	Enable this option to apply default action to all messages.	disable
banned-word {enable disable }	Enable this option to scan banned words for this antispam profile.	disable
bayesian {enable disable }	Enable this option to activate Bayesian scan for this antispam profile.	disable
behavior-analysis {enable disable }	Enable this option to activate behavior analysis scan for this antispam profile.	disable
bayesian-autotraining {enable disable }	Enable to use FortiGuard Antispam and SURBL scan results to train per-user Bayesian databases that are not yet mature (that is, they have not yet been trained with 200 legitimate email and 100 spam in order to recognize spam).	enable
bayesian-user-db {enable disable }	Enable to use per-user Bayesian databases. If disabled, the Bayesian scan will use either the global or the per-domain Bayesian database, whichever is selected for the protected domain.	disable
bayesian-usertraining {enable disable }	Enable to accept email forwarded from email users to the Bayesian control email addresses in order to train the Bayesian databases to recognize spam and legitimate email.	enable
deepheader {enable disable }	Enable to perform extensive inspection of message headers.	disable
deepheader-analysis {enable disable }	Enable to inspect all message headers for known spam characteristics. If the FortiGuard Antispam scan is enabled, this option uses results from that scan, providing up-to-date header analysis.	disable
deepheader-check-ip {enable disable }	Enable to query for the blacklist status of the IP addresses of all SMTP servers appearing in the Received: lines of header lines. If this option is disabled, the FortiMail unit checks only the IP address of the current SMTP client. This option applies only if you have also configured either or both FortiGuard Antispam scan and DNSBL scan.	disable
dict-score <score_int>	Enter the number of dictionary term matches above which the email will be considered to be spam.	
dictionary {enable disable }	Enable to perform a dictionary scan for this profile.	disable

Variable	Description	Default
dnsbl {enable disable }	Enable to perform a DNSBL scan for this profile.	disable
fortiguard-antispam {enable disable }	Enable to let the FortiMail unit query the FortiGuard Antispam service to determine if any of the uniform resource identifiers (URI) in the message body are associated with spam. If any URI is blacklisted, the FortiMail unit considers the email to be spam, and you can select the action that the FortiMail unit will perform.	disable
fortiguard-check-ip {enable disable }	Enable to include whether or not the IP address of the SMTP client is blacklisted in the FortiGuard Antispam query.	disable
fortiguard-phishing-uri {enable disable }	Enable to include whether or not the phishing URI is blacklisted in the FortiGuard Antispam query.	disable
greylist {enable disable }	Enable to perform a greylist scan.	disable
heuristic {enable disable }	Enable to perform a heuristic scan.	disable
heuristic-lower <threshold_int>	Enter the score equal to or below which the FortiMail unit considers an email to not be spam.	-20.000000
heuristic-rules-percent <percentage_int>	<p>Enter the percentage of the total number of heuristic rules that will be used to calculate the heuristic score for an email message.</p> <p>The FortiMail unit compares this total score to the upper and lower level threshold to determine if an email is:</p> <ul style="list-style-type: none"> • spam • not spam • indeterminable (score is between the upper and lower level thresholds) <p>To improve system performance and resource efficiency, enter the lowest percentage of heuristic rules that results in a satisfactory spam detection rate.</p>	100
heuristic-upper {threshold_int}	Enter the score equal to or above which the FortiMail unit considers an email to be spam.	10.000000
image-spam {enable disable }	Enable to perform an image spam scan.	disable
scan-bypass-on-auth {enable disable }	Enable to omit antispam scans when an SMTP sender is authenticated.	disable

Variable	Description	Default
scan-max-size <bytes_int>	Enter the maximum size, in bytes, that the FortiMail unit will scan for spam. Messages exceeding the limit will not be scanned for spam. To scan all email regardless of size, enter 0.	1204 bytes for predefined profiles 600 bytes for user-defined profiles
scan-pdf {enable disable }	Enable to scan the first page of PDF attachments using heuristic, banned word, and image spam scans, if they are enabled.	disable
spam-outbreak-protection {enable disable }	Enable to defer processing a message to allow for FortiGuard servers to be updated or for a FortiSandbox server to supply results to a processing request.	disable
spf-checking {enable disable }	Enable to have the FortiMail unit perform the action configured in this antispam profile, instead of the action configured in the session profile. See “ spf-validation {enable disable} ” on page 242.	disable
surbl {enable disable }	Enable to perform a SURBL scan.	disable
suspicious-newsletter-status {enable disable }	Enable the detection of newsletters.	disable
uri filter {enable disable }	Enable or disable the uniform resource identifiers (URI) profile used by this profile.	disable
uri-filter-status {enable disable }	Enable or disable URI filter scan.	disable
whitelist-enable {enable disable }	Enable to automatically update personal whitelist database from sent email.	disable
whitelist-word {enable disable }	Enable to perform a white list word scan.	disable

Related topics

- [profile antispam-action](#)
- [profile antivirus](#)

profile antispam-action

Use this command to configure antispam action profiles.

Syntax

```
config profile antispam-action
  edit <profile_name>
    set action {discard | none | quarantine | quarantine-review |
               reject | rewrite-rcpt}
    set alternate-host {<relay_fqdn> | <relay_ipv4>}
    set alternate-host-status {enable | disable}
    set archive-account <account_name>
    set archive-status {enable | disable}
    set bcc-addr <recipient_email>
    set bcc-status {enable | disable}
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set notification-profile <profile_name>
    set notification-status {enable | disable}
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
  end
```

Variable	Description	Default
<profile_name>	Enter the name of an antispam action profile.	
action {discard none quarantine quarantine-review reject rewrite-rcpt}	<p>Enter an action for the profile.</p> <ul style="list-style-type: none"> • discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • none: Apply any configured header or subject line tags, if any. • quarantine: Enter to redirect spam to the per-recipient quarantine. For more information, see the FortiMail Administration Guide. This option is available only for incoming profiles. • quarantine-review: Enter to redirect spam to the system quarantine. For more information, see the FortiMail Administration Guide. • reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • rewrite-rcpt: Enter to change the recipient address of any email message detected as spam. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). If you enter this option, also configure rewrite-rcpt-local-type {none prefix replace suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix replace suffix}, and rewrite-rcpt-domain-value <value_str>. 	none
alternate-host {<relay_fqdn> <relay_ipv4>}	<p>Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server.</p> <p>This field applies only if <code>alternate-host-status</code> is enable.</p>	No default.
alternate-host-status {enable disable }	<p>Enable to route the email to a specific SMTP server or relay. Also configure <code>alternate-host {<relay_fqdn> <relay_ipv4>}</code>.</p> <p>Note: If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore <code>mailsetting relay-host-list</code> and the protected domain's <code>tp-use-domain-mta {yes no}</code>.</p>	disable
archive-account <account_name>	<p>Type the email archive account name where you want to archive the spam.</p> <p>Enable <code>archive-status {enable disable}</code> to make this function work.</p> <p>For more information about archive accounts, see “archive account” on page 45.</p>	
archive-status {enable disable }	<p>Enable to allow the <code>archive-account <account_name></code> function to work.</p>	disable

Variable	Description	Default
bcc-addr <recipient_email>	Type the BCC recipient email address. This field applies only if <code>bcc-status</code> is <code>enable</code> .	No default.
bcc-status {enable disable }	Enable to send a blind carbon copy (BCC) of the email. Also configure <code>bcc-addr <recipient_email></code> .	disable
header-insertion- name <name_str>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <p>X-Custom-Header: Detected as spam by profile 22.</p> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See <code>header-insertion-value <header_str></code>.</p>	
header-insertion- status {enable disable }	<p>Enable to add a message header to detected spam.</p> <p>See <code>header-insertion-value <header_str></code>.</p>	disable
header-insertion- value <header_str>	<p>Enter the message header value.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <p>X-Custom-Header: Detected as spam by profile 22.</p> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See <code>header-insertion-name <name_str></code>.</p>	
notification-prof ile <profile_name>	Type the name of the notification profile used for sending notifications.	

Variable	Description	Default
notification-status {enable disable}	Enable sending notifications using a notification profile.	disable
rewrite-rcpt-local-type {none prefix replace suffix}	<p>Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam.</p> <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>. 	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none prefix replace suffix} .	
rewrite-rcpt-domain-type {none-prefix replace suffix}	<p>Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam.</p> <ul style="list-style-type: none"> • none: No change. • prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. • replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. 	none
rewrite-rcpt-domain-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix replace suffix} .	

Related topics

- [profile antispm](#)

profile antivirus

Use this command to create antivirus profiles that you can select in a policy in order to scan email for viruses.

The FortiMail unit scans email header, body, and attachments (including compressed files, such as ZIP, PKZIP, LHA, ARJ, and RAR files) for virus infections. If the FortiMail unit detects a virus, it will take actions as you define in the antivirus action profiles.

Syntax

```
config profile antivirus
  edit <profile_name>
    set action-default { predefined_av_discard |
      predefined_av_reject}
    set action-file-signature
    set action-heuristic
      {predefined_av_discard | predefined_av_reject}
    set action-outbreak
    set action-sandbox-high
    set action-sandbox-low
    set action-sandbox-medium
    set action-sandbox-virus
    set file-signature-check
    set grayware-scan {enable | disable}
    set heuristic {enable | disable}
    set malware-outbreak-protection
    set sandbox-analysis
    set sandbox-analysis-uri
    set sandbox-scan-mode
    set scanner {enable | disable}
  end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
action-default { predefined_av_discard predefined_av_reject }	Type a predefined antivirus action. predefined_av_discard: Accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client. predefined_av_reject: Reject infected email and reply to the SMTP client with SMTP reply code 550.	No default.
action-file-signature	Type a predefined scan for file signature action. predefined_av_discard: predefined_av_reject:	No default.

Variable	Description	Default
action-heuristic {predefined_av_discard predefined_av_reject}	Type a predefined heuristic scanning action on infected email. predefined_av_discard: Accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client. predefined_av_reject: Reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550.	No default.
action-outbreak		
action-sandbox-high	Type to determine the action to take if the FortiSandbox analysis determines that the email messages have viruses or other threat qualities. predefined_av_discard: predefined_av_reject:	No default>
action-sandbox-low	Type to determine the action to take if the FortiSandbox analysis determines that the email messages have viruses or other threat qualities predefined_av_discard: predefined_av_reject:	No default>
action-sandbox-medium	Type to determine the action to take if the FortiSandbox analysis determines that the email messages have viruses or other threat qualities predefined_av_discard: predefined_av_reject:	No default>
action-sandbox-virus	predefined_av_discard: predefined_av_reject:	No default>
file-signature-check	Enable to scan for file signatures.	No default>
grayware-scan {enable disable}	Enable to scan for grayware as well when performing antivirus scanning.	disable
heuristic {enable disable}	Enable to use heuristics when performing antivirus scanning.	disable
malware-outbreak-protection	Instead of using virus signatures, malware outbreak protection uses data analytics from the FortiGuard Service. For example, if a threshold volume of previously unknown attachments are being sent from known malicious sources, they are treated as suspicious viruses. This feature can help quickly identify new threats. Because the infected email is treated as virus, the virus replacement message will be used, if the replacement action is triggered.	No default.

Variable	Description	Default
sandbox-analysis	Enable to send suspicious email attachments to FortiSandbox for inspection. For details about FortiSandbox, see “system fortisandbox” on page 270 .	disable
sandbox-analysis-uri	Enable or disable sending suspicious attachment content to FortiSandbox for analysis.	disable
sandbox-scan-mode	Edits how the email is handled by the FortiSandbox	
scanner {enable disable}	Enable to perform antivirus scanning for this profile.	disable

Related topics

- [profile antispam](#)

profile antivirus-action

Use this command to configure antispam action profiles.

Syntax

```

config profile antivirus-action
edit <profile_name>
    set action {discard | none | quarantine | quarantine-review |
        reject | rewrite-rcpt}
    set alternate-host {<relay_fqdn> | <relay_ipv4>}
    set alternate-host-status {enable | disable}
    set archive-account <account_name>
    set archive-status
    set bcc-addr <recipient_email>
    set bcc-status {enable | disable}
    set deliver-to-original-host
    set header-insertion-name <name_str>
    set header-insertion-status {enable | disable}
    set header-insertion-value <header_str>
    set notification-profile <profile_name>
    set notification-status {enable | disable}
    set replace-infected-status
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
    set rewrite-rcpt-domain-value <value_str>
end

```

Variable	Description	Default
<profile_name>	Enter the name of an antispam action profile.	
action {discard none quarantine-review reject repackage repackage-with-cmsg replace-infected rewrite-rcpt}	<p>Enter an action for the profile.</p> <ul style="list-style-type: none"> • discard: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • none: Apply any configured header or subject line tags, if any. • quarantine-review: Enter to redirect spam to the system quarantine. For more information, see the <i>FortiMail Administration Guide</i>. • reject: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • repackage: Forward the infected email as an attachment but the original email body will still be used without modification. • repackage-with-cmsg: Forward the infected email as an attachment with the customized email body that you define in the custom email template. For example, in the template, you may want to say "The attached email is infected by a virus". • replace-infected: Replaces the infected file with a replacement message that notifies the email user the infected file was removed. You can customize replacement messages. • rewrite-rcpt: Enter to change the recipient address of any email message detected as spam. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol). If you enter this option, also configure <code>rewrite-rcpt-local-type {none prefix replace suffix}</code>, <code>rewrite-rcpt-local-value <value_str></code>, <code>rewrite-rcpt-domain-type {none-prefix replace suffix}</code>, and <code>rewrite-rcpt-domain-value <value_str></code>. 	none
alternate-host {<relay_fqdn> <relay_ipv4>}	<p>Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server.</p> <p>This field applies only if <code>alternate-host-status</code> is <code>enable</code>.</p>	No default.
alternate-host-status {enable disable}	<p>Enable to route the email to a specific SMTP server or relay. Also configure <code>alternate-host {<relay_fqdn> <relay_ipv4>}</code>.</p> <p>Note: If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore <code>mailsetting relay-host-list</code> and the protected domain's <code>tp-use-domain-mta {yes no}</code>.</p>	disable

Variable	Description	Default
archive-account		
archive-status	Enable or disable message archiving.	disable
bcc-addr <recipient_email>	Type the BCC recipient email address. This field applies only if <code>bcc-status</code> is <code>enable</code> .	No default.
bcc-status {enable disable}	Enable to send a blind carbon copy (BCC) of the email. Also configure <code>bcc-addr <recipient_email></code> .	disable
deliver-to-original-host	Enable or disable to option to deliver the message to the original host.	disable
header-insertion-name <name_str>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as spam by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See <code>header-insertion-value <header_str></code>.</p>	
header-insertion-status {enable disable}	<p>Enable to add a message header to detected spam.</p> <p>See <code>header-insertion-value <header_str></code>.</p>	disable
header-insertion-value <header_str>	<p>Enter the message header value.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <pre>X-Custom-Header: Detected as spam by profile 22.</pre> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>See <code>header-insertion-name <name_str></code>.</p>	
notification-profile <profile_name>	Type the name of the notification profile used for sending notifications.	

Variable	Description	Default
notification-status {enable disable}	Enable sending notifications using a notification profile.	disable
replace-infected-status	Enable or disable the option to replace infected body or attachment.	disable
rewrite-rcpt-local-type {none prefix replace suffix}	<p>Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam.</p> <ul style="list-style-type: none"> none: No change. prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>. 	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none prefix replace suffix}.	
rewrite-rcpt-domain-type {none-prefix replace suffix}	<p>Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam.</p> <ul style="list-style-type: none"> none: No change. prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. 	none
rewrite-rcpt-domain-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix replace suffix}.	
subject-tagging-status {enable disable}	Enable to prepend text defined using subject-tagging-text <tag_str> ("tag") to the subject line on detected spam.	disable
subject-tagging-text <tag_str>	Enter the text that will appear in the subject line of the email, such as "[SPAM] ". The FortiMail unit will prepend this text to the subject line of spam before forwarding it to the recipient.	

Related topics

- [profile antivirus](#)

profile authentication

Use this command to configure the FortiMail unit to connect to an external SMTP server in order to authenticate email users.

FortiMail units support the following authentication methods:

- SMTP
- IMAP
- POP3
- RADIUS

When the FortiMail unit is operating in server mode, only local and RADIUS authentication are available.

In addition to authenticating email users for SMTP connections, SMTP profiles can be used to authenticate email users making webmail (HTTP or HTTPS) or POP3 connections to view their per-recipient quarantine.

Depending on the mode in which your FortiMail unit is operating, you may be able to apply authentication profiles through inbound recipient-based policies, IP-based policies, and email user accounts.

For more information, see the [FortiMail Administration Guide](#).

Syntax

```
config profile authentication imap
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication pop3
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set port <port_int>
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication radius
  edit <profile_name>
    set access-override {enable | disable}
    set access-override-attribute <integer>
    set access-override-vendor <integer>
    set auth-prot {auto | chap | mschap | mschap2 | pap}
    set domain-override {enable | disable}
    set domain-override-attribute <integer>
    set domain-override-vendor <integer>
    set nas-ip <ip_addr>
    set port <port_int>
    set secret <password_str>
    set send-domain {enable | disable}
    set server {<fqdn_str> | <host_ipv4>}
config profile authentication smtp
  edit <profile_name>
    set option {ssl secure tls senddomain}
    set server {<fqdn_str> | <host_ipv4>}
    set port <port_int>
    set try-ldap-mailhost {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
access-override {enable disable }	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing access profile.	disable
access-override-a ttribute <integer>	Enter the attribute ID of a vender for remote access permission override. The attribute should hold an access profile name that exists on FortiMail. The default ID is 6, which is Fortinet-Access-Profile.	6
access-override-v endor <integer>	Enter the vender's registered RADIUS ID for remote access permission override. The default ID is 12356, which is Fortinet.	123456

Variable	Description	Default
option {ssl secure tls senddomain}	Enter one or more of the following in a space-delimited list: <ul style="list-style-type: none"> • <code>senddomain</code>: Enable if the IMAP server requires both the user name and the domain when authenticating. • <code>ssl</code>: Enables secure socket layers (SSL) to secure message transmission. • <code>secure</code>: Enables secure authentication. • <code>tls</code>: Enables transport layer security (TLS) to ensure privacy between communicating application 	
port <port_int>	Enter the TCP port number of the IMAP server. The standard port number for IMAP is 143; for SSL-secured IMAP, it is 993.	
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the IMAP server.	
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: <ul style="list-style-type: none"> • <code>domain</code>: Enable if the POP3 server requires both the user name and the domain when authenticating. • <code>ssl</code>: Enables secure socket layers (SSL) to secure message transmission. • <code>secure</code>: Enables secure authentication. • <code>tls</code>: Enables transport layer security (TLS) to ensure privacy between communicating application 	
port <port_int>	Enter the TCP port number of the POP3 server. The standard port number for POP3 is 110; for SSL-secured POP3, it is 995.	
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the POP3 server.	
auth-prot {auto chap mschap mschap2 pap}	Enter the authentication method for the RADIUS server.	auto
domain-override {enable disable }	Enable to override the domain you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing protected domain.	disable
domain-override-a ttribute <integer>	Enter the attribute ID of a vender for remote domain override. The attribute should hold a domain name that exists on FortiMail. The default ID is 3, which is Fortinet-Vdom-Name.	3
domain-override-v endor <integer>	Enter the vender's registered RADIUS ID for remote domain override. The default ID is 12356, which is Fortinet.	123456

Variable	Description	Default
nas-ip <ip_addr>	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiMail interface uses to communicate with the RADIUS server will be applied.	0.0.0.0
port <port_int>	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server. The standard port number for RADIUS is 1812.	1812
secret <password_str>	Enter the password for the RADIUS server.	
send-domain {enable disable }	Enable if the RADIUS server requires both the user name and the domain when authenticating.	
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the RADIUS server.	
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: <ul style="list-style-type: none"> senddomain: Enable if the SMTP server requires both the user name and the domain when authenticating. ssl: Enables secure socket layers (SSL) to secure message transmission. secure: Enables secure authentication. tls: Enables transport layer security (TLS) to ensure privacy between communicating application 	
server {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	
port <port_int>	Enter the TCP port number of the SMTP server. The standard port number for SMTP is 25; for SSL-secured SMTP, it is 465.	
try-ldap-mailhost {enable disable }	Enable if your LDAP server has a mail host entry for the generic user If you select this option, the FortiMail unit will query the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will query the server you entered in the server field.	disable

Related topics

- [profile certificate-binding](#)
- [profile encryption](#)

profile certificate-binding

Use this command to create certificate binding profiles, which establish the relationship between an email address and the certificate that:

- proves an individual's identity
- provides their public (and, for protected domains, private) keys for use with encryption profiles

This relationship and that information can then be used for secure MIME (S/MIME).

If an email is **incoming** to a protected domain and it uses S/MIME encryption, the FortiMail unit compares the sender's identity with the list of certificate bindings to determine if it has a key that can decrypt the email. If it has a matching public key, it will decrypt the email before forwarding it. If it does **not**, it forwards the still-encrypted email to the recipient; the recipient's MUA in that case must support S/MIME and possess the sender's public key.

If an email is **outgoing** from a protected domain, and you have selected an encryption profile in the message delivery rule that applies to the session, the FortiMail unit compares the sender's identity with the list of certificate bindings to determine if it has a certificate and private key. If it has a matching private key, it will encrypt the email using the algorithm specified in the encryption profile. If it does **not**, it performs the failure action indicated in the encryption profile.

Syntax

```
config profile certificate-binding
  edit <profile_id>
    set address-pattern <pattern_str>
    set key-private <key_str>
    set key-public <key_str>
    set key-usage
    set password <pwd_str>
  end
```

Variable	Description	Default
<profile_id>	Enter the ID number of the certificate binding profile.	
address-pattern <pattern_str>	Enter the email address or domain associated with the identity represented by the personal or server certificate.	
key-private <key_str>	Enter the private key associated with the identity, used to encrypt and sign email from that identity.	
key-public <key_str>	Enter the public key associated with the identity, used to encrypt and sign email from that identity.	
key-usage	Use the key for encryption, signing, or both.	encryption
password <pwd_str>	Enter the password for the personal certificate files.	

Related topics

- [profile authentication](#)
- [profile encryption](#)

profile content

Use this command to create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

Unlike antispam profiles, which deal primarily with spam, content profiles match any other type of email.

Content profiles can be used to apply content-based encryption to email. They can also be used to restrict prohibited content, such as words or phrases, file names, and file attachments that are not permitted by your network usage policy. As such, content profiles can be used both for email that you want to protect, and for email that you want to prevent.

Syntax

```
config profile content
  edit <profile_name>
    config attachment-name
      edit attachment-name-pattern <pattern_str>
        set status {enable | disable}
    config monitor
      edit monitor <index_int>
        set action <profile_name>
        set dict-score <score_int>
        set dictionary-group <dictionary-group_name>
        set dictionary-profile <dictionary-profile_name>
        set dictionary-type {group | profile}
        set scan-msoffice {enable | disable}
        set scan-pdf {enable | disable}
```

```

    set status {enable | disable}
set action-default <action_profile>
set action-encrypted <action_profile>
set action-image <action_profile>
set archive-block-on-failure-to-decompress {enable | disable}
set archive-block-password-protected {enable | disable}
set archive-block-recursive {enable | disable}
set archive-content-check {enable | disable}
set archive-max-recursive-level <depth_int>
set attachment-name-disposition {block | pass}
set attachment-type-disposition {block | pass}
set block-msg-fragmented {enable | disable}
set block-msg-without-attachment {enable | disable}
set block-password-protected-doc {enable | disable}
set bypass-on-auth {enable | disable}
set check-max-num-of-attachment {enable | disable}
set defer-message-delivery {enable | disable}
set defersize <threshold_int>
set filetype-application-other {enable | disable}
set filetype-archive {enable | disable}
set filetype-audio {enable | disable}
set filetype-document {enable | disable}
set filetype-document-msoffice {enable | disable}
set filetype-document-msoffice-embedded-check
    {enable | disable}
set filetype-document-msoffice-vba-check {enable | disable}
set filetype-document-openoffice {enable | disable}
set filetype-document-openoffice-embedded-check
    {enable | disable}
set filetype-document-other {enable | disable}
set filetype-document-pdf {enable | disable}
set filetype-document-visio {enable | disable}
set filetype-document-visio-embedded-check {enable | disable}
set filetype-encrypted {enable | disable}
set filetype-encrypted-pgp {enable | disable}
set filetype-encrypted-smime {enable | disable}
set filetype-executable {enable | disable}
set filetype-executable-activex {enable | disable}
set filetype-executable-java {enable | disable}
set filetype-executable-javascript {enable | disable}
set filetype-executable-other {enable | disable}
set filetype-executable-vba {enable | disable}
set filetype-executable-vbs {enable | disable}
set filetype-image {enable | disable}
set filetype-image-gif {enable | disable}
set filetype-image-jpeg {enable | disable}
set filetype-image-other {enable | disable}
set filetype-image-png {enable | disable}
set filetype-image-tiff {enable | disable}

```

```

set filetype-text {enable | disable}
set filetype-text-7bit {enable | disable}
set filetype-text-html {enable | disable}
set filetype-text-other {enable | disable}
set filetype-text-xml {enable | disable}
set filetype-video {enable | disable}
set max-num-of-attachment <integer>
set remove-hidden-html-content {enable | disable}
end

```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	No default.
attachment-name-pattern <pattern_str>	Enter a pattern, such as '*.bat', that matches the email attachment names that you want the content profile to match. The patterns include: <ul style="list-style-type: none"> • *.bat • *.com • *.dll • *.doc • *.exe • *.gz • *.hta • *.ppt • *.rar • *.scr • *.tar • *.tgz • *.vb? • *.wps • *.xl? • *.zip • *.pif 	No default.
status {enable disable }	Enable or disable a pattern that matches the email attachment names that you want the content profile to match.	disable
monitor <index_int>	Enter the index number of the monitor profile. If the monitor profile does not currently exist, it will be created.	No default.
action <profile_name>	Enter the action profile for this monitor profile. The FortiMail unit will perform the actions if the content of the email message matches words or patterns from the dictionary profile that the monitor profile uses.	No default.

Variable	Description	Default
dict-score <score_int>	Enter the number of times that an email must match the content monitor profile before it will receive the action configured in <code>action <profile_name></code> .	1
dictionary-group <dictionary-group_name>	<p>Enter the dictionary profile group that this monitor profile will use.</p> <p>The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profiles. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in <code>action <profile_name></code>.</p> <p>For information on dictionary profiles, see the <i>FortiMail Administration Guide</i>.</p>	No default.
dictionary-profile <dictionary-profile_name>	<p>Enter the dictionary profile that this monitor profile will use.</p> <p>The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profile. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in <code>action <profile_name></code>.</p> <p>For information on dictionary profiles, see the <i>FortiMail Administration Guide</i>.</p>	No default.
dictionary-type {group profile}	Enter <code>profile</code> to detect content based upon a dictionary profile, or <code>group</code> to detect content based upon a group of dictionary profiles. Depending on your selection, also configure either <code>dictionary-group <dictionary-group_name></code> or <code>dictionary-profile <dictionary-profile_name></code> .	group
scan-msoffice {enable disable }	Enable or disable MS Word document scanning for this profile.	disable
scan-pdf {enable disable }	Enable or disable PDF document scanning for this profile.	disable
status {enable disable }	Enable or disable this monitor profile.	disable
action-default <action_profile>	Enter a content action profile to be used by all the content filters except for the encrypted email, which can have its own action. See below for details.	
action-encrypted <action-profile>	For the encrypted email file type, you can use a content action profile to overwrite the <i>default action profile used in the content profile</i> . For example, if you want to redirect encrypted email to a third party box (such as a PGP Universal Server) for decryption, in the content action profile that will be used for the encrypted email, you can enable the option to deliver email to the PGP server as an alternate host.	

Variable	Description	Default
action-image <action_profile>	For the image email file type, you can use a content action profile to overwrite the <i>default action profile used in the content profile</i> .	
archive-block-on-failure-to-decompress {enable disable}	Enter to apply the action configured in “ profile content-action ” on page 198 if an attached archive cannot be successfully decompressed in order to scan its contents.	disable
archive-block-password-protected {enable disable}	Enter to apply the action configured in “ profile content-action ” on page 198 if an attached archive is password-protected.	disable
archive-block-recursive {enable disable}	Enable to block archive attachments whose depth of nested archives exceeds archive-max-recursive-level <depth_int>.	enabled
archive-content-check {enable disable}	Enter to enable consideration of the nesting depth threshold, password protection, and successful decompression when scanning attachments that are archives (such as ZIP, PKZIP, LHA, ARJ, and RAR files).	enabled
archive-max-recursive-level <depth_int>	<p>Enter the nesting depth threshold. Depending upon each attached archive’s depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email.</p> <ul style="list-style-type: none"> • archive-max-recursive-level is 0, or attachment’s depth of nesting equals or is less than archive-max-recursive-level: If the attachment contains a file that matches one of the other MIME file types, perform the action configured for that file type, either block or pass. • Attachment’s depth of nesting is greater than archive-max-recursive-level: Apply the block action, unless you have disabled archive-block-recursive {enable disable}, in which case it will pass the MIME file type content filter. Block actions are specified in the “profile content-action” on page 198. <p>This option applies only if archive-content-check {enable disable} is enabled.</p>	0

Variable	Description	Default
attachment-name-disposition {block pass}	<p>Pass or block email if a file attachment matches the file name patterns enabled in attachment-name-pattern <pattern_str>.</p> <p>If an attachment matches a pattern not enabled, the FortiMail unit will perform the opposite action of whatever you selected, either block or pass.</p> <p>For example, if you enter <code>block</code> and have enabled the name pattern <code>*.exe</code>, files whose names end in <code>.exe</code> will be blocked. All other file names will pass attachment filtering, but will still be subject to any other filters or antispam scans that you have configured.</p> <p>Conversely, if you select <code>pass</code> and enabled <code>*.doc</code>, all file names other than those ending in <code>.doc</code> will be blocked.</p>	block
attachment-type-disposition {block pass}	<p>Block or pass email if a file attachment matches the file types enabled in attachment-type <MIME-type_str>.</p> <p>File types that you have not enabled will receive the action opposite of your block/pass selection.</p> <p>Passed file types will pass attachment file type filtering only, and will still be subject to any other content filters or antispam scans that you have configured.</p>	block
block-msg-fragmented {enable disable}	<p>Enable to detect and block fragmented email.</p> <p>Some mail user agents, such as Outlook, are able to fragment big emails into multiple sub-messages. This is used to bypass oversize limits/scanning</p>	disable
block-msg-without-attachment {enable disable}	Enable to apply the block action configured in the content action profile if an email does not have any attachments.	disable
block-password-protected-doc {enable disable}	Enable to apply the block action configured in the content action profile if an attached MS Office document is password-protected, and therefore cannot be decompressed in order to scan its contents.	disable
bypass-on-auth {enable disable}	Enable to omit antispam scans when an SMTP sender is authenticated.	disable
check-max-num-of-attachment {enable disable}	Enable to specify how many attachments are allowed in one email message. The valid range is between 1 and 100. The default value is 10.	disable
defer-message-delivery {enable disable}	Enable to defer mail delivery from specific senders configured in policy to conserve peak time bandwidth at the expense of sending low priority, bandwidth consuming traffic at scheduled times. For example, you can apply this function to senders of marketing campaign emails or mass mailing.	disable
defersize <threshold_int>	<p>Enter the size threshold in kilobytes. Delivery of email messages greater than this size will be deferred until the period configured for oversize email.</p> <p>To disable deferred delivery, enter 0.</p>	0

Variable	Description	Default
filetype-application-other {enable disable }	Enable to block all file types not specifically described by the other options.	disable
filetype-archive {enable disable }	Enable to block emails that contain archive content to pass the attachment file type filter.	disable
filetype-audio {enable disable }	Enable to block emails that contain audio content to pass the attachment file type filter.	disable
filetype-document {enable disable }	Enable to block emails that contain document content to pass the attachment file type filter.	disable
filetype-document-msoffice {enable disable }	Enable to block emails that contain Microsoft Office content to pass the attachment file type filter.	disable
filetype-document-msoffice-embedded-check {enable disable }	Enable to block emails that contain Microsoft Office content with embedded checking script to pass the attachment file type filter.	disable
filetype-document-msoffice-vba-check {enable disable }	Enable to block emails that contain Microsoft Office content with VBA checking script to pass the attachment file type filter.	disable
filetype-document-openoffice {enable disable }	Enable to block emails that contain OpenOffice content to pass the attachment file type filter.	disable
filetype-document-openoffice-embedded-check {enable disable }	Enable to block emails that contain OpenOffice content with embedded checking script to pass the attachment file type filter.	disable
filetype-document-other {enable disable }	Enable to block emails that contain all other document types not specifically described by the other options to pass the attachment file type filter.	disable
filetype-document-pdf {enable disable }	Enable to block emails that contain PDF content to pass the attachment file type filter.	disable
filetype-document-visio {enable disable }	Enable to block emails that contain Visio content with embedded checking script to pass the attachment file type filter.	disable

Variable	Description	Default
filetype-document -visio-embedded-check {enable disable }	Enable to block emails that contain Visio content with embedded checking script to pass the attachment file type filter.	disable
filetype-encrypted {enable disable }	Enable to block emails that contain encrypted content to pass the attachment file type filter.	disable
filetype-encrypted-pgp {enable disable }	Enable to block emails that contain encrypted PGP content to pass the attachment file type filter.	disable
filetype-encrypted-smime {enable disable }	Enable to block emails that contain encrypted SMIME content to pass the attachment file type filter.	disable
filetype-executable {enable disable }	Enable to block emails that contain executable content to pass the attachment file type filter.	disable
filetype-executable-activex {enable disable }	Enable to block emails that contain Activex executable content to pass the attachment file type filter.	disable
filetype-executable-java {enable disable }	Enable to block emails that contain Java executable content to pass the attachment file type filter.	disable
filetype-executable-javascript {enable disable }	Enable to block emails that contain Java Script executable content to pass the attachment file type filter.	disable
filetype-executable-other {enable disable }	Enable to block emails that contain all other executable content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-executable-vba {enable disable }	Enable to block emails that contain VBA executable content to pass the attachment file type filter.	disable
filetype-executable-vbs {enable disable }	Enable to block emails that contain VBS executable content to pass the attachment file type filter.	disable
filetype-image {enable disable }	Enable to block emails that contain image content to pass the attachment file type filter.	disable

Variable	Description	Default
filetype-image-gif {enable disable }	Enable to block emails that contain GIF image content to pass the attachment file type filter.	disable
filetype-image-jpeg {enable disable }	Enable to block emails that contain JPEG image content to pass the attachment file type filter.	disable
filetype-image-other {enable disable }	Enable to block emails that contain all other image content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-image-png {enable disable }	Enable to block emails that contain PNG image content to pass the attachment file type filter.	disable
filetype-image-tiff {enable disable }	Enable to block emails that contain TIFF image content to pass the attachment file type filter.	disable
filetype-text {enable disable }	Enable to block emails that contain text content to pass the attachment file type filter.	disable
filetype-text-7bit {enable disable }	Enable to block emails that contain 7bit text content to pass the attachment file type filter.	disable
filetype-text-html {enable disable }	Enable to block emails that contain HTML content to pass the attachment file type filter.	disable
filetype-text-other {enable disable }	Enable to block emails that contain all other text content not specifically described by the other options to pass the attachment file type filter.	disable
filetype-text-xml {enable disable }	Enable to block emails that contain XML content to pass the attachment file type filter.	disable
filetype-video {enable disable }	Enable to block emails that contain video content to pass the attachment file type filter.	disable
max-num-of-attachment <integer>	Specify how many attachments are allowed in one email message. The valid range is between 1 and 100. The default value is 10.	10

Variable	Description	Default
<pre>remove-hidden-html-content {enable disable }</pre>	<p>Enable to detect hypertext markup language (HTML) tags and, if found:</p> <ul style="list-style-type: none"> • apply the action profile • add X-FEAS-ATTACHMENT-FILTER: Contains HTML tags. to the message headers <p>This option can be used to mitigate potentially harmful HTML content such as corrupted images or files, or phishing URLs that have been specially crafted for a targeted attack, and therefore not yet identified by the FortiGuard Antispam service.</p> <p>Depending on the action profile, for example, you could warn email users by tagging email that contains potentially dangerous HTML content, or, if you have removed the HTML tags, allow users to safely read the email to decide whether or not it is legitimate first, without automatically displaying and executing potentially dangerous scripts, images, or other files. (Automatic display of HTML content is a risk on some email clients.)</p> <p>Caution: Unless you also select <code>replace</code> for the action in the content action profile, HTML will not be removed, and the email will not be converted to plain text. Instead, the FortiMail unit will only apply whichever other action profile “block” action you have selected.</p> <p>To actually remove HTML tags, you must also select <code>replace</code>.</p>	disable

Variable	Description	Default
	<p>If you select <i>Replace</i>, all HTML tags will be removed, except for the minimum required by the HTML document type definition (DTD):</p> <ul style="list-style-type: none"> • <code><html></code> • <code><head></code> • <code><body></code> <p>Stripped body text will be surrounded by <code><pre></code> tags, which is typically rendered in a monospace font, causing the appearance to mimic plain text.</p> <p>For linked files, which are hosted on an external web site for subsequent download rather than directly attached to the email, the FortiMail unit will download and attach the file to the email before removing the <code></code> or <code><embed></code> tag. In this way, while the format is converted to plain text, attachments and linked files which may be relevant to the content are still preserved.</p> <p>For example, in an email that is a mixture of HTML and plain text (Content-Type: multipart/alternative), and if the action profile's "block" action is <i>replace</i>, the FortiMail unit would remove hyperlink, font, and other HTML tags in the sections labeled with Content-Type: text/html. Linked images would be converted to attachments. (The MIME Content-Type: text/html label itself, however, would not be modified.)</p>	

Related topics

- [profile content-action](#)

profile content-action

Use this command to define content action profiles.

Content action profiles can be used to apply content-based encryption.

Alternatively, content action profiles can define one or more things that the FortiMail unit should do if the content profile determines that an email contains prohibited words or phrases, file names, or file types.

For example, you might have configured most content profiles to match prohibited content, and therefore to use a content action profile named `quar_profile` which quarantines email to the system quarantine for review.

However, you have decided that email that does not pass the dictionary scan named `financial_terms` is **always** prohibited, and should be rejected so that it does not require manual review. To do this, you would first configure a second action profile, named `rejection_profile`, which rejects email. You would then override `quar_profile` specifically for the dictionary-based content scan in each profile by selecting `rejection_profile` for content that matches `financial_terms`.

Syntax

```
config profile content-action
  edit <profile_name>
    set action {discard | encryption | none | quarantine |
      quarantine-review | reject | replace | rewrite-rcpt |
      treat-as-spam}
    set alternate-host {<relay_fqdn> | <relay_ipv4>}
    set alternate-host-status {enable | disable}
    set archive-account <account_name>
    set archive-status {enable | disable}
    set bcc-addr <recipient_email>
    set bcc-status {enable | disable}
    set deliver-to-original-host
    set notification-profile <profile_name>
    set notification-status {enable | disable}
    set encryption-profile <encryption-profile_name>
    set replace-content
    set replace-content-message
    set rewrite-rcpt-domain-type {none | prefix | replace | suffix}
    set rewrite-rcpt-domain-value <case_str>
    set rewrite-rcpt-local-type {none | prefix | replace | suffix}
    set rewrite-rcpt-local-value <value_str>
    set header-insertion-name <text_str>
    set header-insertion-value <value_str>
    set subject-tagging-text <text_str>
    set tagging type {insert-header | tag-subject}
  end
```

Variable	Description	Default
<code><profile_name></code>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
<code>action {discard encryption none quarantine quarantine-review reject replace rewrite-rcpt treat-as-spam}</code>	Enter the action that the FortiMail unit will perform if the content profile determines that an email contains prohibited words or phrases, file names, or file types. <ul style="list-style-type: none"> <code>discard</code>: Accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. <code>encryption</code>: Apply an encryption profile. Also configure encryption-profile <encryption-profile_name>. <code>none</code>: Apply any configured header or subject line tags, if any. <code>quarantine</code>: Divert the email to the per-recipient quarantine. <code>quarantine-review</code>: Divert the email to the system quarantine. <code>reject</code>: Reject the email, replying with an SMTP error code to the SMTP client. <code>replace</code>: Accept the email, but replace the content matching this profile with a replacement message, and, if you have enabled remove-hidden-html-content {enable disable}, strip HTML tags. <code>rewrite-rcpt</code>: Enter to change the recipient address of any email that matches the content profile. Also configure rewrite-rcpt-domain-type {none prefix replace suffix}, rewrite-rcpt-domain-value <case_str>, rewrite-rcpt-local-type {none prefix replace suffix}, and rewrite-rcpt-local-value <value_str>. <code>treat-as-spam</code>: Apply the action selected in the antispam profile. 	replace
<code>alternate-host {<relay_fqdn> <relay_ipv4>}</code>	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if <code>alternate-host-status</code> is <code>enable</code> .	No default.
<code>archive-account <account_name></code>	Type the email archive account name where you want to archive the email. Enable archive-status {enable disable} to make this function work. For more information about archive accounts, see “archive account” on page 45 .	
<code>archive-status {enable disable}</code>	Enable to allow the archive-account <account_name> function to work.	disable

Variable	Description	Default
alternate-host-status {enable disable }	Enable to route the email to a specific SMTP server or relay. Also configure <code>alternate-host {<relay_fqdn> <relay_ipv4>}</code> . Note: If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore <code>mailsetting relay-host-list</code> and the protected domain's <code>tp-use-domain-mta {yes no}</code> .	disable
bcc-addr <recipient_email>	Type the BCC recipient email address. This field applies only if <code>bcc-status</code> is enable.	No default.
bcc-status {enable disable }	Enable to send a blind carbon copy (BCC) of the email. Also configure <code>bcc-addr <recipient_email></code> .	disable
deliver-to-original-host	Enable or disable to deliver to the original host.	disable
notification-profile <profile_name>	Type the name of the notification profile used for sending notifications.	
notification-status {enable disable }	Enable sending notifications using a notification profile.	disable
encryption-profile <encryption-profile_name>	Enter the name of an encryption profile to use.	No default.
replace-content	Enable or disable content replacement.	disable
replace-content-message		
rewrite-rcpt-domain-type {none prefix replace suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email that matches the content profile. <ul style="list-style-type: none">• none: No change.• prefix: Enter to prepend the part with new text. Also configure <code>rewrite-rcpt-domain-value <case_str></code>.• suffix: Enter to append the part with new text. Also configure <code>rewrite-rcpt-domain-value <case_str></code>.• replace: Enter to substitute the part with new text. Also configure <code>rewrite-rcpt-domain-value <case_str></code>.	none
rewrite-rcpt-domain-value <case_str>	Enter the text for the option (except none) you choose in <code>rewrite-rcpt-domain-type {none prefix replace suffix}</code> .	

Variable	Description	Default
<code>rewrite-rcpt-local-type {none prefix replace suffix}</code>	<p>Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email that matches the content profile.</p> <ul style="list-style-type: none"> <code>none</code>: No change. <code>prefix</code>: Enter to prepend the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. <code>suffix</code>: Enter to append the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. <code>replace</code>: Enter to substitute the part with new text. Also configure <code>rewrite-rcpt-local-value <value_str></code>. 	none
<code>rewrite-rcpt-local-value <value_str></code>	Enter the text for the option (except <code>none</code>) you choose in <code>rewrite-rcpt-local-type {none prefix replace suffix}</code> .	
<code>header-insertion-name <text_str></code>	<p>Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.</p> <p>Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client.</p> <p>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:</p> <p><code>X-Content-Filter: Contains banned word.</code></p> <p>If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key.</p> <p>Note: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.</p> <p>Also configure <code>tagging type {insert-header tag-subject}</code>.</p>	
<code>header-insertion-value <value_str></code>	<p>Enter the message header value. The FortiMail unit will add this value to the message header of the email before forwarding it to the recipient.</p> <p>See <code>header-insertion-name <text_str></code>.</p> <p>Also configure <code>tagging type {insert-header tag-subject}</code>.</p>	

Variable	Description	Default
subject-tagging-text <text_str>	Enter the text that will appear in the subject line of the email, such as "[PROHIBITED-CONTENT]". The FortiMail unit will prepend this text to the subject line of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client. Also configure tagging type {insert-header tag-subject} .	
tagging type {insert-header tag-subject}	Enter the type of tagging for this profile. Enter insert-header enables header-insertion-name <text_str> and header-insertion-value <value_str> . Enter tag-subject enables subject-tagging-text <text_str> .	

Related topics

- [profile content](#)

profile dictionary

Use this command to configure dictionary profiles.

Unlike banned words, dictionary terms are UTF-8 encoded, and may include characters other than US-ASCII characters, such as é or ñ.

Dictionary profiles can be grouped or used individually by antispam or content profiles to detect spam, banned content, or content that requires encryption to be applied.

Syntax

```

config profile dictionary
  edit <profile_name>
    config item
      edit <item_int>
        set pattern <pattern_str>
        set pattern-comments <comment_str>
        set pattern-type {ABAROUTING | CANSIN | CUSIP | CreditCard |
          ISIN | USSSN | regex | wildcard}
        set pattern-weight <weight_int>
        set pattern-scan-area {header | body}
        set pattern-status {enable | disable}
        set pattern-max-weight <weight_int>
        set pattern-max-limit {enable | disable}
      end
    end
  end

```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
<item_int>	Enter the index number for the pattern entry where you can add a word or phrase to the dictionary.	

Variable	Description	Default
pattern <pattern_str>	<p>For a predefined pattern, enter a value to change the predefined pattern name.</p> <p>For a use-defined pattern, enter a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression.</p> <p>Regular expressions do not require slash (/) boundaries. For example, enter:</p> <pre>v[i1]agr?a</pre> <p>Matches are case <i>ins</i>sensitive and can occur over multiple lines as if the word were on a single line. (That is, Perl-style match modifier options <i>i</i> and <i>s</i> are in effect.)</p> <p>The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, not the originally encoded string. For example, if the original encoded string is:</p> <pre>=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=</pre> <p>the pattern must match:</p> <pre>Se trata del spam.</pre> <p>Entering the pattern <code>*iso-8859-1*</code> would <i>not</i> match.</p>	
pattern-comments <comment_str>	Enter any description for the pattern.	

Variable	Description	Default
pattern <pattern_str>	<p>For a predefined pattern, enter a value to change the predefined pattern name.</p> <p>For a use-defined pattern, enter a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression.</p> <p>Regular expressions do not require slash (/) boundaries. For example, enter:</p> <pre>v[i1]agr?a</pre> <p>Matches are case <i>ins</i>ensitive and can occur over multiple lines as if the word were on a single line. (That is, Perl-style match modifier options <i>i</i> and <i>s</i> are in effect.)</p> <p>The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, not the originally encoded string. For example, if the original encoded string is:</p> <pre>=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=</pre> <p>the pattern must match:</p> <pre>Se trata del spam.</pre> <p>Entering the pattern <code>*iso-8859-1*</code> would <i>not</i> match.</p>	
pattern-comments <comment_str>	Enter any description for the pattern.	

Variable	Description	Default
pattern <pattern_str>	<p>For a predefined pattern, enter a value to change the predefined pattern name.</p> <p>For a use-defined pattern, enter a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression.</p> <p>Regular expressions do not require slash (/) boundaries. For example, enter:</p> <pre>v[i1]agr?a</pre> <p>Matches are case <i>ins</i>ensitive and can occur over multiple lines as if the word were on a single line. (That is, Perl-style match modifier options <i>i</i> and <i>s</i> are in effect.)</p> <p>The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, not the originally encoded string. For example, if the original encoded string is:</p> <pre>=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=</pre> <p>the pattern must match:</p> <pre>Se trata del spam.</pre> <p>Entering the pattern <code>*iso-8859-1*</code> would <i>not</i> match.</p>	
pattern-comments <comment_str>	Enter any description for the pattern.	

Variable	Description	Default
pattern-type {ABAROUTING CANSIN CUSIP CreditCard ISIN USSSN regex wildcard}	<p>Enter ABAROUTING, CANSIN, CUSIP, CreditCard, ISIN, or USSSN for predefined patterns.</p> <ul style="list-style-type: none"> ABAROUTING: A routing transit number (RTN) is a nine digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which it was drawn. CANSIN: Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666. CUSIP: CUSIP typically refers to both the Committee on Uniform Security Identification Procedures and the 9-character alphanumeric security identifiers that they distribute for all North American securities for the purposes of facilitating clearing and settlement of trades. CreditCard: Major credit card number formats. ISIN: An International Securities Identification Number (ISIN) uniquely identifies a security. Securities for which ISINs are issued include bonds, commercial paper, equities and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at trading and settlement. USSSN: United States Social Security number. The format is a nine digit number, such as 078051111. <p>For user-defined patterns, enter either:</p> <ul style="list-style-type: none"> wildcard: Pattern is verbatim or uses only simple wild cards (? or *). regex: Pattern is a Perl-style regular expression. 	regex
pattern-weight <weight_int>	<p>Enter a number by which an email's dictionary match score will be incremented for each word or phrase it contains that matches this pattern.</p> <p>The dictionary match score may be used by content monitor profiles to determine whether or not to apply the content action.</p>	1
pattern-scan-area {header body}	Enter header to match occurrences of the pattern when it is located in an email's message headers, including the subject line, or body to match occurrences of the pattern when it is located in an email's message body.	
pattern-status {enable disable }	Enable or disable a pattern in a profile.	disable
pattern-max-weight t <weight_int>	Enter the maximum by which matches of this pattern can contribute to an email's dictionary match score.	1
pattern-max-limit {enable disable }	Enable if the pattern must not be able to increase an email's dictionary match score more than the amount configured in pattern-max-weight <weight_int>.	disable

Related topics

- [profile dictionary-group](#)

profile dictionary-group

Use this command to create groups of dictionary profiles.

Dictionary groups can be useful when you want to use multiple dictionary profiles during the same scan.

For example, you might have several dictionaries of prohibited words — one for each language — that you want to use to enforce your network usage policy. Rather than combining the dictionaries or creating multiple policies and multiple content profiles to apply each dictionary profile separately, you could simply group the dictionaries, then select that group in the content monitor profile.

Before you can create a dictionary group, you must first create one or more dictionary profiles. For more information about dictionary profiles, see [“profile dictionary” on page 203](#).

Syntax

```
config profile dictionary-group
  edit <group_name>
    config dictionaries
      edit <dictionary_name>
    end
  end
```

Variable	Description	Default
<group_name>	Enter the name of the dictionary group.	
<dictionary_name>	Enter the dictionary that you want to include in the dictionary group.	

Related topics

- [profile dictionary](#)

profile email-address-group

Use this command to create groups of email addresses.

Email groups include groups of email addresses that are used when configuring access control rules. For information about access control rules, see [“policy access-control receive” on page 152](#).

Syntax

```
config profile email-address-group
  edit <group_name>
    config member
      edit <email_address>
    end
  end
```


Variable	Description	Default
<group_name>	Enter the name of the email address group.	
<email_address>	Enter the email address that you want to include in the email group.	

Related topics

- [policy access-control receive](#)

profile encryption

Use this command to create encryption profiles, which contain encryption settings for secure MIME (S/MIME).

Encryption profiles, unlike other types of profiles, are applied through message delivery rules, not policies.

Syntax

```
config profile encryption
edit <profile_name>
    set encryption-algorithm {aes128 | aes192 | aes256 | cast5 |
        triledes}
    set action-on-failure {drop | send | tls}
    set max-push-size <size_int>
    set protocol {smime | ibe}
    set retrieve-action {push | pull}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the encryption profile.	
encryption-algorithm {aes128 aes192 aes256 cast5 triledes}	Enter the encryption algorithm that will be used with the sender's private key in order to encrypt the email.	aes128
action-on-failure {drop send tls}	Enter the action the FortiMail unit takes when identity-based encryption cannot be used, either: <ul style="list-style-type: none"> • drop: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable. • send: Deliver the email without encryption. 	drop
max-push-size <size_int>	The maximum message size (in KB) of the secure mail delivered (or pushed) to the recipient. Messages that exceed this size are delivered via pull. The size cannot exceed 10240KB. This option applies to the IBE protocol only.	2048

Variable	Description	Default
protocol {smime ibe}	The protocol used for this profile, S/MIME or IBE.	smime
retrieve-action {push pull}	<p>The action used by the mail recipients to retrieve IBE messages.</p> <ul style="list-style-type: none"> push: A notification and a secure mail is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit does not store the message. pull: A notification is delivered to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit stores the message. <p>This option applies to the IBE protocol only.</p>	push

Related topics

- [profile authentication](#)

profile ip-address-group

Use this command to create groups of IP addresses.

IP groups include groups of IP addresses that are used when configuring access control rules. For information about access control rules, see [“policy access-control receive”](#) on page 152.

Syntax

```
config profile ip-address-group
    edit <name>
        config member
            edit <ip/mask>
        end
    end
```

Variable	Description	Default
<name>	Enter the name of the IP address group.	
<ip/mask>	<p>Enter the IP address and netmask that you want to include in the email group. Use the netmask, the portion after the slash (/), to specify the matching subnet.</p> <p>For example, enter 10.10.10.10/24 to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as 10.10.10.0/24 in the access control rule table, with the 0 indicating that any value is matched in that position of the address.</p> <p>Similarly, 10.10.10.10/32 will appear as 10.10.10.10/32 and match only the 10.10.10.10 address.</p> <p>To match any address, enter 0.0.0.0/0.</p>	

Related topics

- [policy access-control receive](#)

profile ip-pool

Use this command to define a range of IP addresses. IP pools can be used in multiple ways:

- To define destination IP addresses of multiple protected SMTP servers if you want to load balance **incoming** email between them
- To define source IP addresses used by the FortiMail unit if you want **outgoing** email to originate from a range of IP addresses.

Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.

For more information, see the [FortiMail Administration Guide](#).

Syntax

```
config profile ip-pool
    edit <profile_name>
        set iprange {enable | disable}
    end
```

Variable	Description	Default
<profile_name>	Enter the name of the IP pool profile.	
iprange {enable disable }	Enter the first and last IP address in each contiguous range included in the profile.	

profile ldap

Use this command to configure LDAP profiles which can query LDAP servers for authentication, email address mappings, and more.

Caution: Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server. When LDAP queries do not match with the server's schema and/or contents, unintended mail processing behaviors can result, including bypassing antivirus scans. For details on preparing an LDAP directory for use with FortiMail LDAP profiles, see the [FortiMail Administration Guide](#).

LDAP profiles each contain one or more queries that retrieve specific configuration data, such as user groups, from an LDAP server.

Syntax

```
config profile ldap
edit <profile_name>
    set access-override {enable | disable}
    set access-override-attribute <attribute_str>
    set address-map-state {enable | disable}
    set alias-base-dn <dn_str>
    set alias-bind-dn <bind_dn_str>
    set alias-bind-password <bindpw_str>
    set alias-dereferencing {never | always | search | find}
    set alias-expansion-level <limit_int>
    set alias-group-expansion-state {enable | disable}
    set alias-group-member-attribute <attribute_str>
    set alias-group-query <query_str>
    set alias-member-mail-attribute <attribute_str>
    set alias-member-query <query_str>
    set alias-schema {activedirectory | dominoperson |
        inetlocalmailrcpt | inetorgperson | userdefined}
    set alias-scope {base one | sub}
    set alias-state {enable | disable}
    set antispam <attribute_str>
    set antivirus <attribute_str>
    set asav-state {enable | disable}
    set auth-bind-dn {cnid | none | searchuser | upn}
    set authstate {enable | disable}
    set base-dn <basedn_str>
    set bind-dn <binddn_str>
    set bind-password <bindpw_str>
    set cache-state {enable | disable}
    set cache-ttl <ttl_int>
    set cnid-name <cnid_str>
    set content <string>
    set dereferencing {never | always | search | find}
    set domain-antispam-attr <attribute_str>
    set domain-antivirus-attr <attribute_str>
    set domain-parent-attr <attribute_str>
    set domain-query <query_str>
    set domain-routing-mail-host-attr <attribute_str>
    set domain-state {enable | disable}
    set external-address <attribute_str>
    set fallback-port <port_int>
    set fallback-server {<fqdn_str> | <server_ipv4>}
    set group-base-dn <basedn_str>
    set group-membership-attribute <attribute_str>
    set group-name-attribute <attribute_str>
    set group-owner {enable | disable}
    set group-owner-address-attribute <attribute_str>
    set group-owner-attribute <attribute_str>
```

```

set group-relative-name {enable | disable}
set group-virtual {enable | disable}
set groupstate {enable | disable}
set internal-address <attribute_str>
set port <port_int>
set query <query_str>
set rcpt-vrfy-bypass {enable | disable}
set routing-mail-host <attribute_str>
set routing-mail-addr <attribute_str>
set routing-state {enable | disable}
set schema {activedirectory | dominoperson | inetlocalmailrcpt |
    inetorgperson | userdefined}
set scope {base | one | sub}
set secure {none | ssl}
set server <name_str>
set timeout <timeout_int>
set unauth-bind {enable | disable}
set upn-suffix <upns_str>
set version {ver2 | ver3}
set webmail-password-change {enable | disable}
set webmail-password-schema {openldap | activedirectory}
end

```

Variable	Description	Default
<profile_name>	Enter the name of the LDAP profile.	
access-override {enable disable }	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing access profile. If there is no match, the specified access profile will still be used. Also specify the access profile attribtue.	disable
access-override-a ttribute <attribute_str>	Specify the access profile attribtue.	
address-map-state {enable disable }	Enable to query the LDAP server defined in the LDAP profile for user objects' mappings between email addresses.	disable

Variable	Description	Default
alias-base-dn <dn_str>	<p>Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for either alias or user objects.</p> <p>User or alias objects should be child nodes of this location.</p> <p>Whether you should specify the base DN of either user objects or alias objects varies by your LDAP schema style. Schema may resolve alias email addresses directly or indirectly (using references).</p> <ul style="list-style-type: none"> • Direct resolution: Alias objects directly contain one or more email address attributes, such as <code>mail</code> or <code>rfc822MailMember</code>, whose values are user email addresses such as <code>user@example.com</code>, and that resolves the alias. The Base DN, such as <code>ou=Aliases,dc=example,dc=com</code>, should contain alias objects. • Indirect resolution: Alias objects do <i>not</i> directly contain an email address attribute that can resolve the alias; instead, in the style of LDAP group-like objects, the alias objects contain only references to user objects that are “members” of the alias “group.” User objects’ email address attribute values, such as <code>user@example.com</code>, actually resolve the alias. Alias objects refer to user objects by possessing one or more “member” attributes whose value is the DN of a user object, such as <code>uid=user,ou=People,dc=example,dc=com</code>. The FortiMail unit performs a first query to retrieve the distinguished names of “member” user objects, then performs a second query using those distinguished names to retrieve email addresses from each user object. The Base DN, such as <code>ou=People,dc=example,dc=com</code>, should contain user objects. 	
alias-bind-dn <bind_dn_str>	<p>Enter the bind DN, such as <code>cn=FortiMailA,dc=example,dc=com</code>, of an LDAP user account with permissions to query the <code>basedn</code>.</p> <p>This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled <code>unauth-bind {enable disable}</code>.</p>	
alias-bind-password <bindpw_str>	<p>Enter the password of <code>alias-bind-dn <bind_dn_str></code>.</p>	
alias-dereferencing {never always search find}	<p>Select the method to use, if any, when dereferencing attributes whose values are references.</p> <ul style="list-style-type: none"> • <code>never</code>: Do not dereference. • <code>always</code>: Always dereference. • <code>search</code>: Dereference only when searching. • <code>find</code>: Dereference only when finding the base search object. 	never

Variable	Description	Default
alias-expansion-level <limit_int>	Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand.	0
alias-group-expansion-state {enable disable}	<p>Enable if your LDAP schema resolves email aliases indirectly. For more information on direct vs. indirect resolution, see alias-base-dn <dn_str>.</p> <p>When this option is disabled, alias resolution occurs using one query. The FortiMail unit queries the LDAP directory using the <code>basedn</code> and the <code>alias-member-query</code>, and then uses the value of each <code>alias-member-mail-attribute</code> to resolve the alias.</p> <p>When this option is enabled, alias resolution occurs using two queries:</p> <ol style="list-style-type: none"> 1 The FortiMail unit first performs a preliminary query using the <code>basedn</code> and <code>alias-group-query</code>, and uses the value of each <code>alias-group-member-attribute</code> as the base DN for the second query. 2 The FortiMail unit performs a second query using the distinguished names from the preliminary query (instead of the <code>basedn</code>) and the <code>alias-member-query</code>, and then uses the value of each <code>alias-member-mail-attribute</code> to resolve the alias. <p>The two-query approach is appropriate if, in your schema, alias objects are structured like group objects and contain references in the form of distinguished names of member user objects, rather than directly containing email addresses to which the alias resolves. In this case, the FortiMail unit must first "expand" the alias object into its constituent user objects before it can resolve the alias email address.</p>	disable
alias-group-member-attribute <attribute_str>	<p>Enter the name of the attribute for the group member, such as <code>member</code>, whose value is the DN of a user object.</p> <p>This attribute must be present in alias objects only if they do not contain an email address attribute specified in alias-member-mail-attribute <attribute_str>.</p>	
alias-group-query <query_str>	<p>Enter an LDAP query filter that selects a set of alias objects, represented as a group of member objects in the LDAP directory.</p> <p>The query filter string filters the result set, and should be based upon any attributes that are common to all alias objects but also exclude non-alias objects.</p> <p>For example, if alias objects in your directory have two distinguishing characteristics, their <code>objectClass</code> and <code>proxyAddresses</code> attributes, the query filter might be:</p> <pre>(&(objectClass=group) (proxyAddresses=smtp:\$m))</pre> <p>where <code>\$m</code> is the FortiMail variable for an email address.</p>	

Variable	Description	Default
alias-member-mail-attribute <attribute_str>	<p>Enter the name of the attribute for the alias member's mail address, such as <code>mail</code> or <code>rfc822MailMember</code>, whose value is an email address to which the email alias resolves, such as <code>user@example.com</code>.</p> <p>This attribute must be present in either alias or user objects, as determined by your schema and whether it resolves aliases directly or indirectly.</p>	
alias-member-query <query_str>	<p>Enter an LDAP query filter that selects a set of either user or email alias objects, whichever object class contains the attribute you configured in alias-member-mail-attribute <attribute_str>, from the LDAP directory.</p> <p>The query filter string filters the result set, and should be based upon any attributes that are common to all user/alias objects but also exclude non-user/alias objects.</p> <p>For example, if user objects in your directory have two distinguishing characteristics, their <code>objectClass</code> and <code>mail</code> attributes, the query filter might be:</p> <pre>(& (objectClass=alias) (mail=\$m))</pre> <p>where <code>\$m</code> is the FortiMail variable for a user's email address.</p>	
alias-schema {activatedirectory dominoperson inetlocalmailrcpt inetorgperson userdefined}	Enter either the name of the LDAP directory's schema, or enter <code>userdefined</code> to indicate a custom schema.	inetorgperson
alias-scope {base one sub}	<p>Enter which level of depth to query:</p> <ul style="list-style-type: none"> <code>base</code>: Query the <code>basedn</code> level. <code>one</code>: Query only the one level directly below the <code>basedn</code> in the LDAP directory tree. <code>sub</code>: Query recursively all levels below the <code>basedn</code> in the LDAP directory tree. 	sub
alias-state {enable disable }	Enable to query user objects for email address aliases.	disable
antispam <attribute_str>	Enter the name of the attribute, such as <code>antispam</code> , whose value indicates whether or not to perform antispam processing for that user.	
antivirus <attribute_str>	Enter the name of the attribute, such as <code>antivirus</code> , whose value indicates whether or not to perform antivirus processing for that user.	
asav-state {enable disable }	Enable to query user objects for mappings between internal and external email addresses.	disable

Variable	Description	Default
auth-bind-dn {cnid none searchuser upn}	<p>Enter either none to not define a user authentication query, or one of the following to define a user authentication query:</p> <ul style="list-style-type: none"> cnid: Enter the name of the user objects' common name attribute, such as <code>cn</code> or <code>uid</code>. searchuser: Enter to form the user's bind DN by using the DN retrieved for that user. upn: Enter to form the user's bind DN by prepending the user name portion of the email address (<code>\$u</code>) to the User Principle Name (UPN, such as <code>example.com</code>). By default, the FortiMail unit will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, also configure <code>upn-suffix</code> <code><upns_str></code>. 	searchuser
authstate {enable disable }	Enable to perform user authentication queries.	disable
base-dn <basedn_str>	<p>Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail unit will search for user objects, such as <code>ou=People,dc=example,dc=com</code>.</p> <p>User objects should be child nodes of this location.</p>	
bind-dn <binddn_str>	<p>Enter the bind DN, such as <code>cn=FortiMailA,dc=example,dc=com</code>, of an LDAP user account with permissions to query the <code>basedn</code>.</p> <p>This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled <code>unauth-bind</code> <code>{enable disable}</code>.</p>	
bind-password <bindpw_str>	Enter the password of <code>bind-dn</code> <code><binddn_str></code> .	
cache-state {enable disable }	<p>Enable to cache LDAP query results.</p> <p>Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiMail unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently.</p> <p>If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of 0 effectively disables caching.</p>	disable
cache-ttl <ttl_int>	<p>Enter the amount of time, in minutes, that the FortiMail unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail unit to query the LDAP server, refreshing the cache.</p> <p>The default TTL value is 1,440 minutes (one day). The maximum value is 10,080 minutes (one week). Entering a value of 0 effectively disables caching.</p>	1440

Variable	Description	Default
cnid-name <cnid_str>	Enter the name of the user objects' common name attribute, such as <code>cn</code> or <code>uid</code> .	
content <string>	<p>Enter the name of the attribute, such as <code>genericContent</code>, whose value is the name of the content profile assigned to the domain.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p> <p>If you do not specify this attribute at all (that is, leave this field blank), the content profile in the matched recipient-based policy will be used.</p>	
dereferencing {never always search find}	<p>Select the method to use, if any, when dereferencing attributes whose values are references.</p> <ul style="list-style-type: none"> <code>never</code>: Do not dereference. <code>always</code>: Always dereference. <code>search</code>: Dereference only when searching. <code>find</code>: Dereference only when finding the base search object. 	never
domain-antispam-attr <attribute_str>	<p>Enter the name of the antispam profile attribute, such as <code>businessCategory</code>, whose value is the name of the antispam profile assigned to the domain.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	
domain-antivirus-attr <attribute_str>	<p>Enter the name of the antivirus profile attribute, such as <code>preferredLanguage</code>, whose value is the name of the antivirus profile assigned to the domain.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	
domain-parent-attr <attribute_str>	<p>Enter the name of the parent domain attribute, such as <code>description</code>, whose value is the name of the parent domain from which a domain inheritate the specific RCPT check settings and quarantine report settings.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	

Variable	Description	Default
domain-query <query_str>	<p>Enter an LDAP query filter that selects a set of domain objects, whichever object class contains the attribute you configured for this option, from the LDAP directory.</p> <p>For details on query syntax, refer to any standard LDAP query filter reference manual.</p> <p>For this option to work, your LDAP directory should contain a single generic user for each domain. The user entry should be configured with attributes to represent the following:</p> <ul style="list-style-type: none"> parent domain from which a domain inherits the specific RCPT check settings and quarantine report settings. For example, <code>description=parent.com</code> IP address of the backend mail server hosting the mailboxes of the domain. For example, <code>mailHost=192.168.1.105</code> antispam profile assigned to the domain. For example, <code>businessCategory=parentAntispam</code> antivirus profile assigned to the domain. For example, <code>preferredLanguage=parentAntivirus</code> 	
domain-routing-mail-host-attr <attribute_str>	<p>Enter the name of the mail host attribute, such as <code>mailHost</code>, whose value is the name of the IP address of the backend mail server hosting the mailboxes of the domain.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	
domain-state {enable disable }	<p>Enable or disable the domain lookup option.</p> <p>For more information about domain lookup, see “domain-query <query_str>” on page 219.</p>	disable
external-address <attribute_str>	<p>Enter the name of the attribute, such as <code>externalAddress</code>, whose value is an email address in the same or another protected domain.</p> <p>This email address will be rewritten into the value of internal-address <attribute_str> according to the match conditions and effects described in Table 8 on page 225.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	extAddress
fallback-port <port_int>	<p>If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number.</p> <p>The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.</p> <p>The FortiMail unit will use SSL-secured LDAP to connect to the server if <code>secure</code> is <code>ssl</code>.</p>	389

Variable	Description	Default
fallback-server {<fqdn_str> <server_ipv4>}	Enter either the fully qualified domain name (FQDN) or IP address of the backup LDAP server. If there is no fallback server, enter an empty string (").	
group-base-dn <basedn_str>	Enter the base DN portion of the group's full DN, such as ou=Groups,dc=example,dc=com. This command applies only if <code>group-relative-name</code> is enable.	
group-membership-attribute <attribute_str>	Enter the name of the attribute, such as <code>memberOf</code> or <code>gidNumber</code> , whose value is the group number or DN of a group to which the user belongs. This attribute must be present in user objects. Whether the value must use common name, group number, or DN syntax varies by your LDAP server schema. For example, if your user objects use both <code>inetOrgPerson</code> and <code>posixAccount</code> schema, user objects have the attribute <code>gidNumber</code> , whose value must be an integer that is the group ID number, such as 10000.	
group-name-attribute <attribute_str>	Enter the name of the attribute, such as <code>cn</code> , whose value is the group name of a group to which the user belongs. This command applies only if <code>group-relative-name</code> is enable.	
group-owner {enable disable }	Enable to query the group object by its distinguished name (DN) to retrieve the DN of the group owner, which is a user that will receive that group's spam reports. Using that user's DN, the FortiMail unit will then perform a second query to retrieve that user's email address, where the spam report will be sent. For more information on sending spam reports to the group owner, see “config domain-setting” on page 81 .	disable
group-owner-address-attribute <attribute_str>	Enter the name of the attribute, such as <code>mail</code> , whose value is the group owner's email address. If <code>group-owner</code> is enable, this attribute must be present in user objects.	
group-owner-attribute <attribute_str>	Enter the name of the attribute, such as <code>groupOwner</code> , whose value is the distinguished name of a user object. You can configure the FortiMail unit to allow that user to be responsible for handling the group's spam report. If <code>group-owner</code> is enable, this attribute must be present in group objects.	

Variable	Description	Default
group-relative-name {enable disable }	<p>Enable to specify the base distinguished name (DN) portion of the group's full distinguished name (DN) in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query.</p> <p>For example, you might find it more convenient in each recipient-based policy to type only the group name, <code>admins</code>, rather than typing the full DN, <code>cn=admins,ou=Groups,dc=example,dc=com</code>. In this case, you could enable this option, then <code>basedn (ou=Groups,dc=example,dc=com)</code> and <code>groupnameattribute (cn)</code>. When performing the query, the FortiMail unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the <code>groupnameattribute</code> and the <code>basedn</code> configured in the LDAP profile.</p> <p>Note: Enabling this option is appropriate only if your LDAP server's schema specifies that the group membership attribute's value must use DN syntax. It is not appropriate if this value uses another type of syntax, such as a number or common name.</p> <p>For example, if your user objects use both <code>inetOrgPerson</code> and <code>posixAccount</code> schema, user objects have the attribute <code>gidNumber</code>, whose value must be an integer that is the group ID number, such as <code>10000</code>. Because a group ID number does not use DN syntax, you would not enable this option.</p>	disable
group-virtual {enable disable }	<p>Enable to use objects within the base DN of <code>base-dn <basedn_str></code> as if they were members of a user group object.</p> <p>For example, your LDAP directory might not contain user group objects. In that sense, groups do not really exist in the LDAP directory. However, you could mimic a group's presence by enabling this option to treat all users that are child objects of the base DN in the user object query as if they were members of such a group.</p>	disable
groupstate {enable disable }	Enable to perform LDAP group queries.	disable
internal-address <attribute_str>	<p>Enter the name of the LDAP attribute, such as <code>internalAddress</code>, whose value is an email address in the same or another protected domain.</p> <p>This email address will be rewritten into the value of <code>external-address <attribute_str></code> according to the match conditions and effects described in Table 8 on page 225.</p> <p>The name of this attribute may vary by the schema of your LDAP directory.</p>	intAddress

Variable	Description	Default
port <port_int>	<p>If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number.</p> <p>The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.</p>	389
query <query_str>	<p>Enter an LDAP query filter, enclosed in single quotes ('), that selects a set of user objects from the LDAP directory.</p> <p>The query filter string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects.</p> <p>For example, if user objects in your directory have two distinguishing characteristics, their <code>objectClass</code> and <code>mail</code> attributes, the query filter might be:</p> <pre>(& (objectClass=inetOrgPerson) (mail=\$m))</pre> <p>where <code>\$m</code> is the FortiMail variable for a user's email address.</p> <p>If the email address (<code>\$m</code>) as it appears in the message header is different from the user's email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the user by the email address (<code>\$m</code>) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract "-spam" from the end of the user name portion of the recipient email address, you could use the query filter:</p> <pre>(& (objectClass=inetOrgPerson) (mail=\$m\${-spam}))</pre> <p>where <code>\${-spam}</code> is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract "spam-" from the beginning of the user name portion of the recipient email address, you could use the query filter:</p> <pre>(& (objectClass=inetOrgPerson) (mail=\$m\${^spam-}))</pre> <p>where <code>\${^spam-}</code> is the FortiMail variable for the tag to remove before performing the query.</p> <p>For some schemas, such as Microsoft Active Directory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure an alias query to resolve aliases.</p> <p>For details on query syntax, refer to any standard LDAP query filter reference manual.</p> <p>This command applies only if <code>schema</code> is <code>userdefined</code>.</p>	<pre>(& (objectClass=inetOrgPerson) (mail=\$m))</pre>

Variable	Description	Default
<code>rcpt-vrfy-bypass</code> {enable disable}	If you have selected using LDAP server to verify recipient address and your LDAP server is down, enabling this option abandons recipient address verification and the FortiMail unit will continue relaying email.	disable
<code>routing-mail-host</code> <attribute_str>	Enter the name of the LDAP attribute, such as <code>mailHost</code> , whose value is the fully qualified domain name (FQDN) or IP address of the email server that stores email for the user's email account.	mailHost
<code>routing-mail-addr</code> <attribute_str>	<p>Enter the name of the LDAP attribute, such as <code>mailRoutingAddress</code>, whose value is the email address of a deliverable user on the email server, also known as the mail host.</p> <p>For example, a user may have many aliases and external email addresses that are not necessarily known to the email server. These addresses would all map to a real email account (mail routing address) on the email server (mail host) where the user's email is actually stored.</p> <p>A user's recipient email address located in the envelope or header portion of each email will be rewritten to this address.</p>	mailRoutingAddress
<code>routing-state</code> {enable disable}	Enable to perform LDAP queries for mail routing.	disable
<code>schema</code> {activedirectory dominoperson inetlocalmailrcpt inetorgperson userdefined}	<p>Enter either the name of the LDAP directory's schema, or enter <code>userdefined</code> to indicate a custom schema.</p> <p>If you enter <code>userdefined</code>, you must configure <code>query</code>.</p>	inetorgperson
<code>scope</code> {base one sub}	<p>Enter which level of depth to query:</p> <ul style="list-style-type: none"> <code>base</code>: Query the <code>basedn</code> level. <code>one</code>: Query only the one level directly below the <code>basedn</code> in the LDAP directory tree. <code>sub</code>: Query recursively all levels below the <code>basedn</code> in the LDAP directory tree. 	sub
<code>secure</code> {none ssl}	<p>Enter a value to indicate whether or not to connect to the LDAP server(s) using an encrypted connection.</p> <ul style="list-style-type: none"> none: Use a non-secure connection. SSL: Use an SSL-secured (LDAPS) connection. <p>Note: If your FortiMail unit is deployed in server mode, and you want to enable webmail-password-change {enable disable} using an LDAP server that uses a Microsoft ActiveDirectory-style schema, you must select SSL. ActiveDirectory servers require a secure connection for queries that change user passwords.</p>	none
<code>server</code> <name_str>	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.	

Variable	Description	Default
timeout <timeout_int>	Enter the maximum amount of time in seconds that the FortiMail unit will wait for query responses from the LDAP server.	10
unauth-bind {enable disable }	<p>An unauthenticated bind is a bind where the user supplies a user name with no password. Some LDAP servers (such as Active Directory) allow unauthenticated bind by default. For better security, FortiMail does not accept empty password when doing LDAP authentication even if the backend LDAP server allows it.</p> <p>In some cases, such as allowing all members of a distribution list to access their quarantined email in gateway and transparent mode, this option needs to be enabled in the LDAP profile, so that FortiMail can accept LDAP authentication requests with empty password (user name must not be empty), and forward such requests to the backend LDAP server. If unauthenticated bind is permitted by the LDAP server, AND if the user exists on the server, FortiMail will consider authentication successful and grant access to the user.</p> <p>It is highly recommended that a dedicated LDAP profile (with this option enabled) is used for the above case. All other users should use separate LDAP profiles with this option disabled (this is the default setting) to maintain maximum security.</p> <p>Note: This option is available in CLI only. And it only takes effect for webmail access in gateway and transparent mode.</p>	disable
upn-suffix <upns_str>	If you want to use a UPN other than the mail domain, enter that UPN. This can be useful if users authenticate with a domain other than the mail server's principal domain name.	
version {ver2 ver3}	Enter the version of the protocol used to communicate with the LDAP server.	ver3
webmail-password-change {enable disable }	Enable to perform password change queries for FortiMail webmail users.	disable
webmail-password-schema {openldap activedirectory}	<p>Enter one of the following to indicate the schema of your LDAP directory:</p> <ul style="list-style-type: none"> openldap: The LDAP directory uses an OpenLDAP-style schema. activedirectory: The LDAP directory uses a Microsoft Active Directory-style schema. <p>Note: Microsoft Active Directory requires that password changes occur over an SSL-secured connection.</p>	openldap

Email address mapping

Address mappings are bidirectional, one-to-one or many-to-many mappings. They can be useful when:

- you want to hide a protected domain’s true email addresses from recipients
- a mail domain’s domain name is not globally DNS-resolvable, and you want to replace the domain name with one that is
- you want to rewrite email addresses

Like aliases, address mappings translate email addresses. They do not translate many email addresses into a single email address. However, *unlike* aliases:

- Mappings cannot translate one email address into many.
- Mappings cannot translate an email address into one that belongs to an unprotected domain. (This restriction applies to locally defined address mappings only. This is not enforced for mappings defined on an LDAP server.)
- Mappings are applied bidirectionally, when an email is outgoing as well as when it is incoming to the protected domain.
- Mappings may affect both sender and recipient email addresses, and may affect those email addresses in both the message envelope and the message header, depending on the match condition.

The following table illustrates the sequence in which parts of each email are compared with address mappings for a match, and which locations’ email addresses are translated if a match is found.

Note: Both `RCPT TO:` and `MAIL FROM:` email addresses are always evaluated for a match with an address mapping. If both `RCPT TO:` and `MAIL FROM:` contain email addresses that match the mapping, both mapping translations will be performed.

Table 8: Match evaluation and rewrite behavior for email address mappings

Order of evaluation	Match condition	If yes...	Rewrite to...
---------------------	-----------------	-----------	---------------

Table 8: Match evaluation and rewrite behavior for email address mappings

1	Does <code>RCPT TO:</code> match an external email address?	Replace <code>RCPT TO:</code> .	Internal email address
2	Does <code>MAIL FROM:</code> match an internal email address?	<p>For each of the following, if it matches an internal email address, replace it:</p> <ul style="list-style-type: none"> • <code>MAIL FROM:</code> • <code>RCPT TO:</code> • <code>From:</code> • <code>To:</code> • <code>Return-Path:</code> • <code>Cc:</code> • <code>Reply-To:</code> • <code>Return-Receipt-To:</code> • <code>Resent-From:</code> • <code>Resent-Sender:</code> • <code>Delivery-Receipt-To:</code> • <code>Disposition-Notification-To:</code> 	External email address

For example, you could create an address mapping between the internal email address `user1@marketing.example.net` and the external email address `sales@example.com`. The following effects would be observable on the simplest case of an outgoing email and an incoming reply:

- **For email from `user1@marketing.example.net` to others:** `user1@marketing.example.net` in both the message envelope (`MAIL FROM:`) and many message headers (`From:`, etc.) would then be replaced with `sales@example.com`. Recipients would only be aware of the email address `sales@example.com`.
- **For email to `sales@example.com` from others:** The recipient address in the message envelope (`RCPT TO:`), but **not** the message header (`To:`), would be replaced with `user1@marketing.example.net`. `user1@marketing.example.net` would be aware that the sender had originally sent the email to the mapped address, `sales@example.com`.

Alternatively, you can configure an LDAP profile to query for email address mappings.

Related topics

- [profile authentication](#)

profile notification

Use this command configure a notification profile.

Syntax

```
config profile notification
  edit <profile_name>
    set attach-original-message {enable | disable}
    set email-template <template_name>
    set other <recipient_address>
    set recipient {none | other | recipient | sender}
    set type {generic | sender_addr_rate_ctrl}
  end
```

Variable	Description	Default
<profile_name>	Enter the name of the notification profile.	
attach-original-message {enable disable}	Enable to include the original message as attachment in the notification email.	disable
email-template <template_name>	Specify the email template to use.	default
other <recipient_addresses>	Specify the recipient address for the notification email.	
recipient {none other recipient sender}	Specify who you want to send the notification to.	none
type {generic sender_addr_rate_ctrl}		generic

profile resource

Use this command configure a resource profile.

Note: This command only applies in the server mode.

Syntax

```
config profile resource
  edit <profile_name>
    set auto-check-message
    set auto-delete-old-mail <days>
    set auto-delete-sent-folder <days>
    set auto-delete-trash-folder <days>
    set mobile-access {enable | disable}
    set outbound-whitelist
    set quarantine-bcc-addr
    set quarantine-bcc-status
    set quarantine-days
    set quarantine-report
    set quota <number_mb>
    set release-auto-whitelist
    set release-through-email
    set release-through-web
    set status {enable | disable}
    set webmail-access {enable | disable}
    set webmail-addressbook-access {domain | none | system}
  end
```

Variable	Description	Default
auto-check-message	Enable or disable auto checking new messages in webmail.	disable
<profile_name>	Enter the name of the notification profile.	
auto-delete-old-mail <days>	Enter the number of days after which the FortiMail unit will automatically delete email that is locally hosted. 0 means not to delete email.	0
auto-delete-sent-folder <days>	Enter the number of days after which the FortiMail unit will automatically delete email in the sent folder. 0 means not to delete email.	0
auto-delete-trash-folder <days>	Enter the number of days after which the FortiMail unit will automatically empty the trash folder. 0 means not to delete email.	14
mobile-access {enable disable}	Enable to allow mobile users to access their email via webmail.	enable
outbound-whitelist	Enable or disable automatically updating personal white lists from sent emails.	disable
quarantine-bcc-addr		
quarantine-bcc-status	Enable or disable bcc messages to specified emails when quarantined emails released.	disable
quarantine-days	Enter the number of days a quarantined message is kept. Enter 0 for indefinitely.	
quarantine-report	Generates a summary report of the quarantined emails.	
quota <number_mb>	Enter the user's disk space quota in Megabytes.	200

Variable	Description	Default
release-auto-whitelist	Automatically add sender of a released message to personal white list.	
release-through-email	Enable or disable auto release quarantined emails through email	disable
release-through-web	Enable or disable auto release quarantined emails through the web.	disable
status {enable disable}	Enable or disable the user account.	enable
webmail-access {enable disable}	Enable or disable user's webmail access.	enable
webmail-addressbook-access {domain none system}	Enable or disable user access to system and/or domain address book.	domain
webmail-user-preference {enable disable}	Use this command to turn on/off the user preference option on the webmail.	enable

profile session

Use this command to create session profiles.

While, like antispam profiles, session profiles protect against spam, session profiles focus on the connection and envelope portion of the SMTP session, rather than the message header, body, or attachments.

Similar to access control rules or delivery rules, session profiles control aspects of sessions in an SMTP connection.

Syntax

```
config profile session
  edit <profile_name>
    set block_encrypted {enable | disable}
    set bypass-bounce-verification {enable | disable}
    set check-client-ip-quick {enable | disable}
    set conn-blacklisted {enable | disable}
    set conn-concurrent <connections_int>
    set conn-hiden {enable | disable}
    set conn-idle-timeout <timeout_int>
    set conn-total <connections_int>
    set dkim-signing {enable | disable}
    set dkim-signing-authenticated-only {enable | disable}
    set dkim-validation {enable | disable}
    set domain-key-validation {enable | disable}
    set domain-key-validation {enable | disable}
    set email-queue {default | incoming | no-preference | outgoing}
    set endpoint-reputation {enable | disable}
    set endpoint-reputation-action {reject | monitor}
    set endpoint-reputation-blacklist-duration <duration_int>
    set endpoint-reputation-blacklist-trigger <trigger_int>
    set eom-ack {enable | disable}
    set error-drop-after <errors_int>
    set error-penalty-increment <penalty-increment_int>
    set error-penalty-initial <penalty-initial_int>
    set error-penalty-threshold <threshold_int>
    set limit-NOOPs <limit_int>
    set limit-RSETs <limit_int>
    set limit-email <limit_int>
    set limit-helo <limit_int>
    set limit-max-header-size <limit_int>
    set limit-max-message-size <limit_int>
    set limit-recipient <limit_int>
    set mail-route <profile_name>
    set number-of-messages <limit_int>
    set number-of-recipients <limit_int>
    set recipient-blacklist-status {enable | disable}
    set recipient-rewrite-map <profile_name>
    set recipient-whitelist-status {enable | disable}
    set remote-log <profile_name>
    set remove-headers {enable | disable}
    set remove-received-headers {enable | disable}
    set sender-blacklist-status {enable | disable}
    set sender-reputation-reject-score <threshold_int>
    set sender-reputation-status {enable | disable}
    set sender-reputation-tempfail-score <threshold_int>
    set sender-reputation-throttle-number <rate_int>
    set sender-reputation-throttle-percentage <percentage_int>
```

```

set sender-reputation-throttle-score <threshold_int>
set sender-reputation-throttle-number <num_integer>
set sender-reputation-throttle-percentage <percentage_int>
set sender-reputation-throttle-score <threshold_int>
set sender-whitelist-status {enable | disable}
set session-3way-check {enable | disable}
set session-allow-pipelining {no | loose | strict}
set session-command-checking {enable | disable}
set session-disallow-encrypted {enable | disable}
set session-helo-char-validation {enable | disable}
set session-helo-domain-check {enable | disable}
set session-helo-rewrite-clientip {enable | disable}
set session-helo-rewrite-custom {enable | disable}
set session-helo-rewrite-custom-string <helo_str>
set session-prevent-open-relay {enable | disable}
set session-recipient-domain-check {enable | disable}
set session-reject-empty-domain {enable | disable}
set session-sender-domain-check {enable | disable}
set spf-validation {enable | disable}
set splice-status {enable | disable}
set splice-threshold
set splice-unit {seconds | kilobytes}
config header-removal-list
    edit <key_str>
config recipient-blacklist
    edit <recipient_address_str>
config recipient-whitelist
    edit <recipient_address_str>
config sender-blacklist
    edit <sender_address_str>
config sender-whitelist
    edit <sender_address_str>
next
end

```

Variable	Description	Default
<profile_name>	Enter the name of the session profile.	
<key_str>	Enter a header key to remove it from email messages.	
<recipient_addresses_str>	Enter a blacklisted recipient email address to which this profile is applied.	
<recipient_addresses_str>	Enter a whitelisted recipient email address to which this profile is applied.	
<sender_address_str>	Enter a blacklisted sender email address to which this profile is applied.	
<sender_address_str>	Enter a whitelisted sender email address to which this profile is applied.	

Variable	Description	Default
<code>block_encrypted</code> {enable disable }	<p>Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam.</p> <p>Disable to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable
<code>bypass-bounce-ver</code> <code>ification</code> {enable disable }	<p>Select to, if bounce verification is enabled, omit verification of bounce address tags on incoming bounce messages.</p> <p>This bypass does not omit bounce address tagging of outgoing email.</p> <p>Alternatively, you can omit bounce verification according to the protected domain. For details, see “config domain-setting” on page 81.</p> <p>For information on enabling bounce address tagging and verification (BATV), see “antispam bounce-verification key” on page 29.</p>	disable
<code>check-client-ip-q</code> <code>uick</code> {enable disable }	<p>Enable to query the FortiGuard Antispam Service to determine if the IP address of the SMTP server is blacklisted. This action will happen during the connection phase.</p> <p>In an antispam profile, you can also enable FortiGuard black IP checking. But that action happens after the entire message has been received by FortiMail.</p> <p>Therefore, if this feature is enabled in a session profile and the action is reject, the performance will be improved.</p>	disable
<code>conn-blacklisted</code> {enable disable }	<p>Enable to prevent clients from using SMTP servers that have been blacklisted in antispam profiles or, if enabled, the FortiGuard AntiSpam service.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable
<code>conn-concurrent</code> <connections_int>	<p>Enter a limit to the number of concurrent connections per SMTP client. Additional connections are rejected.</p> <p>To disable the limit, enter 0.</p>	0

Variable	Description	Default
conn-hidden {enable disable }	<p>Enter either of the following transparency behaviors:</p> <ul style="list-style-type: none"> enable: Be transparent. Preserve the IP address or domain name in: the SMTP greeting (HELO/EHLO) in the envelope, the <code>Received:</code> message headers of email messages, and the IP addresses in the IP header. This masks the existence of the FortiMail unit. disable: Do not be transparent. Replace the IP addresses or domain names with that of the FortiMail unit. <p>This option applies only if the FortiMail unit is operating in transparent mode. For more information about the proxies and built-in MTA transparency, see the FortiMail Administration Guide.</p> <p>Note: Unless you have enabled <code>exclusive {enable disable}</code> in “policy ip” on page 160, the <code>hide (tp-hidden {no yes})</code> option in “config domain-setting” on page 81 has precedence over this option, and may prevent it from applying to incoming email messages.</p> <p>Note: For full transparency, also set the <code>hide (tp-hidden {no yes})</code> option in “config domain-setting” on page 81 to <code>yes</code>.</p>	disable
conn-idle-timeout <timeout_int>	<p>Enter a limit to the number of seconds a client may be inactive before the FortiMail unit drops the connection.</p> <p>For server mode, gateway mode, and transparent MTA mode, 0 means the default value 30 seconds.</p> <p>For transparent proxy mode, 0 means no limit.</p>	30
conn-rate-number <connections_int>	<p>This is a rate limit to the number of messages sent per client IP address per time interval (the default value is 30 minutes).</p> <p>You set the time interval using the command: <code>config antispam settings set session-profile-rate-control-interval <minutes></code>.</p> <p>To disable the limit, enter 0.</p>	0
conn-total <connections_int>	<p>Enter a limit to the total number of concurrent connections from all sources.</p> <p>To disable the limit, enter 0.</p>	0
dkim-signing {enable disable }	<p>Enable to sign outgoing email with a DKIM signature.</p> <p>This option requires that you first generate a domain key pair and publish the public key in the DNS record for the domain name of the protected domain. If you do not publish the public key, destination SMTP servers will not be able to validate your DKIM signature. For details on generating domain key pairs and publishing the public key, see the FortiMail Administration Guide.</p>	disable

Variable	Description	Default
<code>dkim-signing-authenticated-only</code> {enable disable}	Enable to sign outgoing email with a DKIM signature only if the sender is authenticated. This option is available only if <code>dkim-signing</code> is enable.	disable
<code>dkim-validation</code> {enable disable}	Enable to, if a DKIM signature is present, query the DNS server that hosts the DNS record for the sender's domain name to retrieve its public key to decrypt and verify the DKIM signature. An invalid signature increases the client sender reputation score and affect the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DKIM information or the message is not signed, the FortiMail unit omits the DKIM signature validation.	disable
<code>domain-key-validation</code> {enable disable}	Enable to, if the DNS record for the domain name of the sender lists DomainKeys authorized IP addresses, compare the client IP address to the IP addresses of authorized senders. An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score. If the DNS record for the domain name of the sender does not publish DomainKeys information, the FortiMail unit omits the DomainKeys client IP address validation.	disable
<code>email-addr-rewrite-options</code> {envelope-from envelope-from-as-key envelope-to header-from header-to reply-to}	Specify which sender and recipient addresses to rewrite. For more details, see the session profile section in the FortiMail Administration Guide.	
<code>email-queue</code> {default incoming no-preference outgoing}	Enter the email queue to use for the matching sessions.	no-preference
<code>endpoint-reputation</code> {enable disable}	Enable to accept, monitor, or reject email based upon endpoint reputation scores. This option requires that your RADIUS server provide mappings between dynamic IP addresses and MSISDNs/subscriber IDs to the FortiMail unit. If this profile governs sessions of SMTP clients with static IP addresses, instead consider <code>sender-reputation-status</code> {enable disable}.	disable

Variable	Description	Default
endpoint-reputation-action {reject monitor }	Enter either: <ul style="list-style-type: none"> reject: Reject email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed <i>Auto blacklist score trigger value</i>. monitor: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed <i>endpoint-reputation-blacklist-trigger value</i>. Log entries appear in the history log. 	reject
endpoint-reputation-blacklist-duration <duration_int>	Enter the number of minutes that an MSISDN/subscriber ID will be prevented from sending email or MMS messages after they have been automatically blacklisted.	0
endpoint-reputation-blacklist-trigger <trigger_int>	Enter the MSISDN reputation score over which the FortiMail unit will add the MSISDN/subscriber ID to the automatic blacklist. The trigger score is relative to the period of time configured as the automatic blacklist window.	5
eom-ack {enable disable }	Enable to acknowledge the end of message (EOM) signal immediately after receiving the carriage return and line feed (CRLF) characters that indicate the EOM, rather than waiting for antispam scanning to complete. If the FortiMail unit has not yet completed antispam scanning by the time that four (4) minutes has elapsed, it will return SMTP reply code 451(Try again later), resulting in no permanent problems, as according to RFC 2281, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail unit to acknowledge the EOM command. Enabling this option prevents those rare cases.	disable
error-drop-after <errors_int>	Enter the total number of errors the FortiMail unit will accept before dropping the connection.	5
error-penalty-increment <penalty-increment_int>	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.	1
error-penalty-initial <penalty-initial_int>	Enter the delay penalty in seconds for the first error after the number of "free" errors is reached.	1
error-penalty-threshold <threshold_int>	Enter the number of number of errors permitted before the FortiMail unit will penalize the SMTP client by imposing a delay.	1
limit-NOOPs <limit_int>	Enter the limit of NOOP commands that are permitted per SMTP session. Some spammers use NOOP commands to keep a long session alive. Legitimate sessions usually require few NOOPs. Enter 0 to reset to the default value.	10

Variable	Description	Default
limit-RSETs <limit_int>	Enter the limit of RSET commands that are permitted per SMTP session. Some spammers use RSET commands to try again after receiving error messages such as unknown recipient. Legitimate sessions should require few RSETs. To disable the limit, enter 0.	20
limit-email <limit_int>	Enter the limit of email messages per session to prevent mass mailing. To disable the limit, enter 0.	10
limit-helo <limit_int>	Enter the limit of SMTP greetings that a connecting SMTP server or client can perform before the FortiMail unit terminates the connection. Restricting the number of SMTP greetings allowed per session makes it more difficult for spammers to probe the email server for vulnerabilities, as a greater number of attempts results in a greater number of terminated connections, which must then be re-initiated. Enter 0 to reset to the default value.	3
limit-max-header-size <limit_int>	Enter the limit of the message header size. If enabled, messages with headers over the threshold size are rejected.	32
limit-max-message-size <limit_int>	Enter the limit of message size. If enabled, messages over the threshold size are rejected. Note: If both this option and <code>max-message-size <limit_int></code> in the protected domain are enabled, email size will be limited to whichever size is smaller.	10240
limit-recipient <limit_int>	Enter the limit of recipients to prevent mass mailing.	500
mail-route <profile_name>	Enter a mail routing profile to be used in a session profile.	
number-of-messages <limit_int>	Enter the number of message per client per time interval (the default value is 30 minutes). You set the time interval using the command: <code>config antisпам settings set session-profile-rate-control-interval <minutes></code> . Enter 0 to disable the limit.	0
number-of-recipients <limit_int>	Enter the number of recipients per client per time interval (the default value is 30 minutes). You set the time interval using the command: <code>config antisпам settings set session-profile-rate-control-interval <minutes></code> . Enter 0 to disable the limit.	0
recipient-blacklist-status {enable disable }	Enable to use an envelope recipient (RCPT TO:) black list in SMTP sessions to which this profile is applied, then define blacklisted email addresses using <code><recipient_address_str></code> .	disable

Variable	Description	Default
recipient-rewrite-map <profile_name>	Enter an address rewrite profile to be used in a session profile.	
recipient-whitelist-status {enable disable}	Enable to use an envelope recipient (RCPT TO:) white list in SMTP sessions to which this profile is applied, then define whitelisted email addresses using <recipient_address_str>.	disable
remote-log <profile_name>	Enter a remote logging profile. Note that the remote logging profiles used here are the same as the system-wide remote logging profiles.	
remove-headers {enable disable}	Enable to remove other configured headers from email messages.	disable
remove-received-headers {enable disable}	Enable to remove all Received: message headers from email messages.	disable
sender-blacklist-status {enable disable}	Enable to use an envelope sender (MAIL FROM:) black list in SMTP sessions to which this profile is applied, then define the blacklisted email addresses using <sender_address_str>.	disable
sender-reputation-reject-score <threshold_int>	Enter a sender reputation score over which the FortiMail unit will return a rejection error code when the SMTP client attempts to initiate a connection. This option applies only if sender-reputation-status {enable disable} is enable.	80
sender-reputation-status {enable disable}	Enable to reject email based upon sender reputation scores.	disable
sender-reputation-tempfail-score <threshold_int>	Enter a sender reputation score over which the FortiMail unit will return a temporary failure error code when the SMTP attempts to initiate a connection. This option applies only if sender-reputation-status {enable disable} is enable.	55
sender-reputation-throttle-number <rate_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client.	5
sender-reputation-throttle-percentage <percentage_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client, as a percentage of the number of email messages that the sender sent during the previous hour.	1

Variable	Description	Default
sender-reputation-throttle-score <threshold_int>	<p>Enter the sender reputation score over which the FortiMail unit will rate limit the number of email messages that can be sent by this SMTP client.</p> <p>The enforced rate limit is either <code>sender-reputation-throttle-number</code> <rate_int> or <code>sender-reputation-throttle-percentage</code> <percentage_int>, whichever value is greater.</p> <p>This option applies only if <code>sender-reputation-status</code> {enable disable} is enable.</p>	15
sender-reputation-throttle-number <num_integer>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client.	5
sender-reputation-throttle-percentage <percentage_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client, as a percentage of the number of email messages that the SMTP client sent during the previous hour.	1
sender-reputation-throttle-score <threshold_int>	<p>Enter a sender reputation score over which the FortiMail unit will rate limit the number of email messages that can be sent by this SMTP client.</p> <p>Entering 0 means no score limit and thus no action. But FortiMail still monitors the sender reputation and increases or decreases the sender reputation scores accordingly.</p>	35
sender-whitelist-status {enable disable}	Enable to use an envelope sender (MAIL FROM:) white list in SMTP sessions to which this profile is applied, then define whitelisted email addresses using <sender_address_str>.	disable
session-3way-check {enable disable}	<p>Enable to reject the email if the domain name in the SMTP greeting (HELO/EHLO) and recipient email address (RCPT TO:) match, but the domain name in the sender email address (MAIL FROM:) does not.</p> <p>Mismatching domain names is sometimes used by spammers to mask the true identity of their SMTP client.</p> <p>This check only affects unauthenticated sessions.</p>	disable
session-allow-pipelining {no loose strict}	<p>Select one of the following behaviors for ESMTP command pipelining, which causes some SMTP commands to be accepted and processed as a batch, increasing performance over high-latency connections.</p> <ul style="list-style-type: none"> <code>no</code>: Disabled. The FortiMail unit accepts only one command at a time during an SMTP session and will not accept the next command until it completes processing of the previous command. <code>loose</code>: Enabled, and does not require strict compliance with RFC2920. <code>strict</code>: Enabled, but requires strict compliance with RFC 2920. <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	no

Variable	Description	Default
<pre>session-command-checking {enable disable }</pre>	<p>Enable to return SMTP reply code 503, rejecting the SMTP command, if the client or server uses SMTP commands that are syntactically incorrect.</p> <p>EHLO or HELO, MAIL FROM:, RCPT TO: (can be multiple), and DATA commands must be in that order. AUTH, STARTTLS, RSET, NOOP commands can arrive at any time. Other commands, or commands in an unacceptable order, return a syntax error.</p> <p>In the following example, the invalid commands are highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:41:15 GMT EHLO example.com 250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you RCPT TO:<user1@example.com> 503 5.0.0 Need MAIL before RCPT</pre>	disable
<pre>session-disallow-encrypted {enable disable }</pre>	<p>Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam.</p> <p>Clear to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable

Variable	Description	Default
<pre>session-helo-char-validation {enable disable }</pre>	<p>Enable to return SMTP reply code 501, rejecting the SMTP greeting, if the client or server uses a greeting that contains a domain name with invalid characters.</p> <p>To avoid disclosure of a real domain name, spammers sometimes spoof an SMTP greeting domain name with random characters, rather than using a genuine, valid domain name. If this option is enabled, such connections are rejected.</p> <p>In the following example, the invalid command is highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT EHLO ^^&^^#\$ 501 5.0.0 Invalid domain name</pre> <p>Valid characters for domain names include:</p> <ul style="list-style-type: none"> • alphanumerics (A to Z and 0 to 9) • brackets ([and]) • periods (.) • dashes (-) • underscores (_) • number symbols(#) • colons (:) 	disable
<pre>session-helo-domain-check {enable disable }</pre>	<p>Enable to return SMTP reply code 501, rejecting the SMTP greeting, if the client or server uses a greeting that contains a domain name with invalid characters.</p> <p>To avoid disclosure of a real domain name, spammers sometimes spoof an SMTP greeting domain name with random characters, rather than using a genuine, valid domain name. If this option is enabled, such connections are rejected.</p> <p>In the following example, the invalid command is highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT EHLO ^^&^^#\$ 501 5.0.0 Invalid domain name</pre> <p>Valid domain characters include:</p> <ul style="list-style-type: none"> • alphanumerics (A to Z and 0 to 9) • brackets ([and]) • periods (.) • dashes (-) • underscores (_) • number symbols(#) • colons (:) 	disable

Variable	Description	Default
session-helo-rewrite-clientip {enable disable }	<p>Enable to rewrite the HELO/EHLO domain to the IP address of the SMTP client to prevent domain name spoofing.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable
session-helo-rewrite-custom {enable disable }	<p>Enable to rewrite the HELO/EHLO domain, then enter the replacement text using session-helo-rewrite-custom-string <helo_str>.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable
session-helo-rewrite-custom-string <helo_str>	Enter the replacement text for the HELO/EHLO domain.	
session-prevent-open-relay {enable disable }	<p>Enable to block unauthenticated outgoing connections to unprotected mail servers in order to prevent clients from using open relays to send email. If clients from your protected domains are permitted to use open relays to send email, email from your domain could be blacklisted by other SMTP servers.</p> <p>This feature:</p> <ul style="list-style-type: none"> • applies only if the FortiMail unit is operating in transparent mode • only affects unauthenticated sessions, and • is applicable only if you allow clients to use an unprotected SMTP server for outgoing connections. For details, see “mailsetting proxy-smtp” on page 144. 	disable
session-recipient-domain-check {enable disable }	<p>Enable to return SMTP reply code 550, rejecting the SMTP command, if the domain name portion of the recipient address is not a domain name that exists in either MX or A records.</p> <p>In the following example, the invalid command is highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:48:32 GMT EHLO example.com 250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you MAIL FROM:<user1@fortinet.com> 250 2.1.0 <user1@fortinet.com>... Sender ok RCPT TO:<user2@example.com> 550 5.7.1 <user2@example.com>... Relaying denied. IP name lookup failed [192.168.1.1]</pre> <p>This check only affects unauthenticated sessions.</p>	disable

Variable	Description	Default
<pre>session-reject-empty-domain {enable disable }</pre>	<p>Enable to return SMTP reply code 553, rejecting the SMTP command, if a domain name does not follow the "@" symbol in the sender email address.</p> <p>Because the sender address is invalid and therefore cannot receive delivery status notifications (DSN), you may want to disable this feature.</p> <p>In the following example, the invalid command is highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2007 14:48:32 GMT EHLO example.com 250-FortiMail-400.localdomain Hello [192.168.171.217], pleased to meet you MAIL FROM:<john@> 553 5.1.3 <john@>... Hostname required This check only affects unauthenticated sessions.</pre>	disable
<pre>session-sender-domain-check {enable disable }</pre>	<p>Enable to return SMTP reply code 421, rejecting the SMTP command, if the domain name portion of the sender address is not a domain name that exists in either MX or A records.</p> <p>In the following example, the invalid command is highlighted in bold:</p> <pre>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT EHLO 250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you MAIL FROM:<user1@example.com> 421 4.3.0 Could not resolve sender domain.</pre>	disable
<pre>spf-validation {enable disable }</pre>	<p>Enable to, if the sender domain DNS record lists SPF authorized IP addresses, compare the client IP address to the IP addresses of authorized senders in the DNS record.</p> <p>An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score.</p> <p>If the DNS record for the domain name of the sender does not publish SPF information, the FortiMail unit omits the SPF client IP address validation.</p>	disable

Variable	Description	Default
splice-status {enable disable }	<p>Enable to permit splicing.</p> <p>Splicing enables the FortiMail unit to simultaneously scan an email and relay it to the SMTP server. This increases throughput and reduces the risk of a server timeout.</p> <p>If the FortiMail unit detects spam or a virus, it terminates the server connection and returns an error message to the sender, listing the spam or virus name and infected file name.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	disable
splice-threshold <integer>	<p>Enter a threshold value to switch to splice mode based on time (seconds) or data size (kilobytes) using splice-unit {seconds kilobytes}.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	0
splice-unit {seconds kilobytes}	<p>Enter the time (seconds) or data size (kilobytes) for the splice threshold.</p> <p>This option applies only if the FortiMail unit is operating in transparent mode.</p>	seconds

Related topics

- [profile content](#)

profile tls

Use this command to configure TLS profiles that can be used by receive rules (also called access control rules) and delivery rules.

Syntax

```
config profile tls
  edit <profile_name>
    set level {encrypt | none | secure | preferred}
    set action {fail | tempfail}
  end
```

Variable	Description	Default
<profile_name>	Enter the name of the tls profile.	
level {encrypt none secure preferred}	Enter the security level of the TLS connection. <ul style="list-style-type: none"> • encrypt: Requires a basic TLS connection. Failure to negotiate a TLS connection results in the connection being rejected according to the <code>action</code> setting. • none: Disables TLS. Requests for a TLS connection will be ignored. • preferred: Allow a simple TLS connection, but do not require it. Data is not encrypted, nor is the identity of the server validated with a certificate. • secure: Requires a certificate-authenticated TLS connection. CA certificates must be installed on the FortiMail unit before they can be used for secure TLS connections. For information on installing CA certificates, see the FortiMail Administration Guide. 	preferred
action {fail tempfail}	Select the action the FortiMail unit takes when a TLS connection cannot be established. <ul style="list-style-type: none"> • fail • tempfail This option does not apply for profiles whose <code>level</code> is preferred.	tempfail

Related topics

- [policy access-control receive](#)

report

Use this command to configure report profiles that define what information will appear in generated reports.

In addition to log files, FortiMail units require a report profile to be able to generate a report. A report profile is a group of settings that contains the report name, file format, subject matter, and other aspects that the FortiMail unit considers when generating the report.

Syntax

```
config report
edit <profile_name>
    set dest-ip-mask <ip/netmask_str>
    set dest-ip-type {ip-group | ip-mask}
    set direction {both | incoming | outgoing}
    set domains {all | <protected-domain_str>}
    set file-format {html | pdf}
    set period-relative {last-2-weeks | last-7-days | last-14-days |
        last-30-days | last-N-days | last-N-hours | last-N-weeks |
        last-month | last-quarter | last-week | not-used |
```

```

        this-month | this-quarter | this-week | this-year | today |
        yesterday}
set period-relative-value <n_int>
set query-status <query_str>
set recipients <recipient_str>
set schedule {daily | dates | none | weekdays}
set schedule-dates <dates_str>
set schedule-hour <time_int>
set schedule-weekdays <days_str>
set sender-domains
end

```

Variable	Description	Default
<profile_name>	Enter the name of the report profile.	
dest-ip-mask <ip/netmask_str>	Enter the IP address to which reports on logged email messages are destitined.	0.0.0.0/32
dest-ip-type {ip-group ip-mask}	Enter the type of the IP address for sending reports on logged email messages.	ip-mask
direction {both incoming outgoing}	Enter one of the following: <ul style="list-style-type: none"> both: Report on both incoming and outgoing email. incoming: Report only on email whose recipient is a member of a protected domain. outgoing: Report only on email whose recipient is not a member of a protected domain. 	both
domains {all <protected-domain _str>}	Enter either ALL to include all protected domains in the report, or enter a list of one or more protected domains. Separate each protected domain with a comma (,).	all
file-format {html pdf}	Enter the file format of the generated report.	pdf
period-relative {last-2-weeks last-7-days last-14-days last-30-days last-N-days last-N-hours last-N-weeks last-month last-quarter last-week not-used this-month this-quarter this-week this-year today yesterday}	Enter the time span of log messages from which to generate the report. If you entered last-N-days, last-N-hours, or last-N-weeks also configure period-relative-value <n_int>.	
period-relative-v alue <n_int>	If you entered last-N-days, last-N-hours, or last-N-weeks as the value for period-relative, enter the value of n.	

Variable	Description	Default
query-status <query_str>	Enter the name of a query whose result you want to include in the report, such as Mail_Stat_Viruses. To display a list of available query names, enter a question mark (?)	
recipients <recipient_str>	Enter a list of one or more recipient email addresses that will receive the report generated from the report profile. Separate each recipient with a comma (,).	
schedule {daily dates none weekdays}	Enter a value to schedule when the report is automatically generated, or to disable generating reports on schedule if you want to initiate them only manually. <ul style="list-style-type: none"> daily: Generate the report every day. dates: Generate the report on certain dates in the month. Also configure schedule-dates <dates_str>. none: If you do not want to automatically generate the report according to a schedule, enter none. You can still manually initiate the FortiMail unit to generate a report at any time. weekdays: Generate the report on certain days of the week. Also configure schedule-weekdays <days_str>. 	
schedule-dates <dates_str>	Enter the dates to generate the reports. Separate each date with a comma (,). For example, to generate a report on the first and fourteenth of each month, you would enter 1, 14.	
schedule-hour <time_int>	If you want to automatically generate the report according to a schedule, enter the hour of the day, according to a 24-hour clock, at which you want to generate the report. Also configure the days on which you want to generate the report. For example, to generate reports at 5 PM, you would enter 17.	
schedule-weekdays <days_str>	Enter the days to generate the reports. Separate each day with a comma (,). For example, to generate a report on Friday and Wednesday, you would enter wednesday, friday.	
sender-domains	Enter the selected sender domain names (empty means ALL)	

Related topics

- [log alertemail setting](#)

sensitive data

Use this command to configure sensitive data.

Syntax

```
config sensitive-data fingerprint
  edit <fingerprint data name>
    config document
      edit <document id>
        set filename
        set signature
config sensitive-data fingerprint-source
  edit <DLP server name>
    set file-path
    set file-pattern
    set keep-modified
    set password
    set period
    set remove-deleted
    set scan-subdirectories
    set server
    set server-type
    set username
  edit linux
    set file-path
    set file-pattern
    set keep-modified
    set password
    set period
    set remove-deleted
    set scan-subdirectories
    set server
    set server-type
    set username
end
```

Variable	Description	Default
<fingerprint data name>	Enter the name of the fingerprint data you want to configure.	
document	Enter to examine a list of created document ids.	
<document id>	Enter the name of the document you want to modify.	
filename	Enter the filename of the fingerprint document.	
signature	Enter the signature of the file.	
fingerprint-source	Enter to configure the fingerprint source.	
<DLP server name>	Enter the name of the DLP server.	
linux	Enter the linux identifier.	
file-path	Enter the file path on the server.	
file-pattern	Enter the file patterns to fingerprint.	

Variable	Description	Default
keep-modified	Keep previous fingerprints for modified files (Enable/Disable)	
password	Enter the login password.	
period	Select periodic server checking.	
remove-deleted	Remove fingerprints for deleted files (Enable/Disable).	
scan-subdirectories	Fingerprint files in subdirectories (Enable/Disable).	
server	Enter the IP address of the server.	
server-type	Enter the DLP server type.	
username	Enter the login username.	

system accprofile

Use this command to configure access profiles that, in conjunction with the domain to which an administrator account is assigned, govern which areas of the web-based manager and CLI that an administrator can access, and whether or not they have the permissions necessary to change the configuration or otherwise modify items in each area.

Syntax

```
config system accprofile
  edit <profile_name>
    set archive {none | read | read-write}
    set black-white-list {none | read | read-write}
    set greylist {none | read | read-write}
    set others {none | read | read-write}
    set personal-quarantine {none | read | read-write}
    set policy {none | read | read-write}
    set system {none | read | read-write}
    set system-quarantine {none | read | read-write}
  end
```

Variable	Description	Default
<profile_name>	Enter the name of the access profile.	
archive {none read read-write}	For the archiving configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
black-white-list {none read read-write}	For the black and white list configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
greylist {none read read-write}	For the grelist configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
others {none read read-write}	For the rest of the configurations except policy, black-white-list, and quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile.	none

Variable	Description	Default
personal-quarantine {none read read-write}	For personal quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
policy {none read read-write}	For the policy configuration, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
system {none read read-write}	For system settings, enter the permissions that will be granted to administrator accounts associated with this access profile.	none
system-quarantine {none read read-write}	For system quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile.	none

Related topics

- [system admin](#)

system admin

Use this command to configure FortiMail administrator accounts.

By default, FortiMail units have a single administrator account, `admin`. For more granular control over administrative access, you can create additional administrator accounts that are restricted to being able to configure a specific protected domain and/or with restricted permissions. For more information, see the [FortiMail Administration Guide](#).

Syntax

```
config system admin
    edit <name_str>
        set access-profile <profile_name>
        set auth-strategy {ldap | local | local-plus-radius | pki | radius}
        set is-system-domain {no | yes}
        set language <lang_str>
        set ldap-profile <profile_name>
        set password <password_str>
        set pkuser <pkuser_str>
        set radius-permission-check {enable | disable}
        set radius-profile <profile_int>
        set radius-subtype-id <subtype_int>]
        set radius-vendor-id <vendor_int>
        set sshkey <key_str>
        set status {enable | disable}
        set trusthosts <host_ipv4mask>
        set webmode (basic | advanced)
    end
```

Variable	Description	Default
<name_str>	Enter the name of the administrator account.	
access-profile <profile_name>	Enter the name of an access profile that determines which functional areas the administrator account may view or affect.	
auth-strategy {ldap local local-plus-radius pki radius}	Select the local or remote type of authentication that the administrator will be able to use: <ul style="list-style-type: none"> • ldap • local • radius • radius-plus-local • pki 	local
is-system-domain {no yes}	Enter yes to indicate that the administrator account may view all settings on the FortiMail unit.	yes
language <lang_str>	Enter this administrator account's preference for the display language of the web-based manager. Available languages vary by whether or not you have installed additional language resource files. To view a list of languages, enter a question mark (?).	english
ldap-profile <profile_name>	If auth-strategy is ldap , enter the LDAP profile you want to use.	
password <password_str>	If auth-strategy is local or radius-plus-local , enter the password for the administrator account. Caution: Do not enter a FortiMail administrator password less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiMail unit.	
pkiuser <pkiuser_str>	If auth-strategy is pki , enter the name of a PKI user. Whether the administrator is required to log in only with a valid personal certificate or password-style authentication fallback is allowed varies by your configuration of pki-mode { enable disable }.	
radius-permission-check {enable disable}	If auth-strategy is local or radius-plus-local , enable to query the RADIUS server for the permissions attribute.	disable
radius-profile <profile_int>	If auth-strategy is local or radius-plus-local , enter the index number of a RADIUS authentication profile.	
radius-subtype-id <subtype_int>]	If auth-strategy is local or radius-plus-local , and radius-permission-check is enable , enter the RADIUS subtype identifier.	0
radius-vendor-id <vendor_int>	If auth-strategy is local or radius-plus-local , and radius-permission-check is enable , enter the RADIUS vendor identifier.	0

Variable	Description	Default
sshkey <key_str>	Enter the SSH key string surrounded in single straight quotes ('). When connecting from an SSH client that presents this key, the administrator will not need to provide their account name and password in order to log in to the CLI.	
status {enable disable}	Enable to activate the admin user.	disable
trusthosts <host_ipv4mask>	Enter one to three IP addresses and netmasks from which the administrator can log in to the FortiMail unit. Separate each IP address and netmask pair with a comma (,). To allow the administrator to authenticate from any IP address, enter 0.0.0.0/0.0.0.0.	0.0.0.0 /0.0.0.0 0
webmode (basic advanced)	Enter which display mode will initially appear when the administrator logs in to the web-based manager. The administrator may switch the display mode during their session; this affects only the initial state of the display.	basic

Related topics

- [sensitive data](#)

system appearance

Use this command to customize the appearance of the web-based manager, FortiMail webmail, and per-recipient quarantine of the FortiMail unit.

Syntax

```
config system appearance
    set customized-login-status {enable | disable}
    set fallback-charset <language_code>
    set login-page-language <lang_str>
    set login-page-theme
    set product <product-name_str>
    set webmail-help-status {enable | disable}
    set webmail-help-url <url_str>
    set webmail-lang <language_str>
    set webmail-login <login_str>
    set webmail-login-hint <login_hint_str>
    set webmail-theme {IndigoDarkBlue | RedGrey | Standard}
    set webmail-theme-status {enable | disable}
end
```

Variable	Description	Default
customized-login-status {enable disable}	Enable to edit a graphic that will appear at the top of all webmail pages. The image's dimensions must be 314 pixels wide by 36 pixels tall.	disable
fallback-charset <language_code>	Enter the fallback charset for non RFC2047 compliant message.	english
login-page-language <lang_str>	Enter the default language for the display of the login page of the web-based manager. To view a list of languages, enter a question mark (?). Note that the setting only affect the login page, not the entire web-based manager.	english
login-page-theme	Enter the default display theme of the login page.	
product <product-name_str>	Enter the text that will precede 'Administrator Login' on the login page of the web-based manager.	FortiMail
webmail-help-status {enable disable}	Enable to display the help button in the webmail interface. The default help contents are provided by Fortinet.	Enable
webmail-help-url <url_str>	If you want to provide your own help to the webmail users, you can enter the URL of the help file.	
webmail-lang <language_str>	Enter the name of the language in English, such as 'French', that will be used when an email user initially logs in to FortiMail webmail/per-recipient quarantine. The email user may switch the display language in their preferences; this affects only the initial state of the display. Available languages vary by whether or not you have installed additional language resource files.	English
webmail-login <login_str>	Enter a word or phrase that will appears on top of the webmail login page, such as Webmail Login.	Login
webmail-login-hint <login_hint_str>	Enter a hint for the user name, such as Your Email Address. This hint will appear as a mouse-over display on the login name field.	address
webmail-theme {IndigoDarkBlue RedGrey Standard}	Select a theme for the webmail GUI.	RedGrey
webmail-theme-status {enable disable}	Enable or disable webmail theme change.	enable

Related topics

- [system global](#)

system backup-restore-mail

Use this command to configure backup and restoration of email user's mailboxes.

For the initial backup, whether manually or automatically initiated, the FortiMail unit will make a full backup. For subsequent backups, the FortiMail unit will make the number of incremental backups, then make another full backup, and repeat this until it reaches the maximum number of full backups to keep on the backup media, which you selected in `full <full-backups_int>`. At that point, it will overwrite the oldest full backup.

For example, if `full <full-backups_int>` is 3 and `monthly-incremental-days` is 4, the FortiMail unit would make a full backup, then 4 incremental backups. It would repeat this two more times for a total of 3 backup sets, and then overwrite the oldest full backup when creating the next backup.

Syntax

```
config system backup-restore-mail
  set encryption-key <key>
  set folder <path_str>
  set full <full-backups_int>
  set host <fortimail-fqdn_str>
  set hour-of-day <hours_int>
  set monthly-day-of-month
  set monthly-incremental-days
  set number-of-backups
  set port <port_int>
  set protocol {ext-usb | ext-usb-auto | iscsi_server | nfs |
               smb-winserver | ssh}
  set status {enable | disable}
end
```

Variable	Description	Default
encryption-key <key>	Enter the encryption key for backup/restore.	
folder <path_str>	Enter the path of the folder on the backup server where the FortiMail unit will store the mailbox backups, such as: /home/fortimail/mailboxbackups This field appears only if the backup media is an NFS server or SSH server.	FortiMail-mail-data-backup
full <full-backups_int>	Enter the total number of full backups to keep on the backup media. Valid values are between 1 and 10.	3
host <fortimail-fqdn_str>	If you want to restore all mailboxes from a backup labeled with the fully qualified domain name (FQDN) of a previous FQDN, or that of another FortiMail unit, enter the FQDN of the backup that you want to restore. For example, to restore the most recent backup made by a FortiMail unit named fortimail.example.com, enter fortimail.example.com.	

Variable	Description	Default
hour-of-day <hours_int>	Enter the hour of the day, according to a 24-hour clock, on the days of the week at which to make backups. For example, to make backups at 9 PM, enter 21.	23
monthly-day-of-month	Enter the day of the month to perform the full backup.	
monthly-incremental-days	Enter how often to perform the monthly incremental backup.	
number-of-backups	Enter the number of full backups to keep.	
port <port_int>	Enter the TCP port number on which the backup server listens for connections. This field does not appear if the backup media is a USB disk.	22
protocol {ext-usb ext-usb-auto iscsi_server nfs smb-winserver ssh}	Enter one of the following types of backup media: <ul style="list-style-type: none"> ext-usb: An external hard drive connected to the FortiMail unit's USB port. ext-usb-auto: An external disk connected to the FortiMail unit's USB port. Unlike the previous option, this option only creates a backup when you connect the USB disk, or when you manually initiate a backup rather than according to a schedule. iscsi_server: An Internet SCSI (Small Computer System Interface), also called iSCSI, server. nfs: A network file system (NFS) server. smb/winserver: A Windows-style file share. ssh: A server that supports secure shell (SSH) connections. Other available options vary by your choice of backup media.	nfs
status {enable disable }	Enable to allow backups and restoration to occur, whether manually initiated or automatically performed on schedule. Also configure the backup media in <code>protocol {ext-usb ext-usb-auto iscsi_server nfs smb-winserver ssh}</code> and, if applicable to the type of the media, configure a schedule in <code>encryption-key <key></code> and <code>hour-of-day <hours_int></code> . Note: You should enable backups/restoration <i>after</i> configuring the other options if a scheduled backup will occur before you configure <code>protocol {ext-usb ext-usb-auto iscsi_server nfs smb-winserver ssh}</code> . Failure to do so would result in a failed backup attempt, requiring you to wait for the failed attempt to terminate before you can continue to configure this feature.	disable

Related topics

- [system mailserver](#)

system central-management

Use this command to enable FortiManager support.

Note: Latest FortiManager releases support centralized management of FortiMail v3.0 MR4 and MR5 releases. For FortiMail v4.0 releases, centralized management is supported in FortiManager v4.2 and later releases. Refer to FortiManager release notes for details about supported FortiMail versions. For information on configuring a FortiManager unit to manage or provide services to your other Fortinet brand devices, see the [FortiManager Administration Guide](#).

In addition to configuration backup and remote administration, enabling FortiManager support allows your FortiMail unit to retrieve firmware image files.

In addition to enabling FortiManager support on the FortiMail unit, you must also register the device with the FortiManager unit's device list in order to indicate that it has permission to connect. For details, see the [FortiMail Administration Guide](#).

Syntax

```
config system central-management
    set allow-push-configuration {enable | disable}
    set auto-backup {enable | disable}
    set ip <fortimanager_ipv4>
    set status {enable | disable}
end
```

Variable	Description	Default
allow-push-configuration {enable disable}	Enable to accept configuration changes from the FortiManager unit. This command applies only if <code>status</code> is <code>enable</code> and <code>ip</code> is configured.	disable
auto-backup {enable disable}	Enable to automatically send a configuration revision to the FortiManager unit when a FortiMail administrator logs out, if the configuration has changed. When configuration revisions are stored on a FortiManager unit, you can revert to any previous revision by using the command “restore config” on page 344 . This command applies only if <code>central-management</code> is <code>enable</code> and <code>ip</code> is configured.	disable
ip <fortimanager_ipv4>	Enter the IP address of the FortiManager unit. This command applies only if <code>central-management</code> is <code>enable</code> .	0.0.0.0
status {enable disable}	Enable to enable FortiManager support. Also configure <code>ip <fortimanager_ipv4></code> , <code>auto-backup {enable disable}</code> , and <code>allow-push-configuration {enable disable}</code> . Caution: On the FortiManager unit, verify that the FortiMail unit has been registered with its device list. Failure to register the FortiMail unit may cause inability of the FortiMail unit to connect to the FortiManager unit.	disable

system certificate ca

Use this command to import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.

CA certificates are required by connections that use transport layer security (TLS). For more information, see the *FortiMail Administration Guide*.

Syntax

```
config system certificate ca
  edit <name_str>
    set certificate <cert_str>
  end
```

Variable	Description	Default
<name_str>	Enter a name for this certificate.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	

Related topics

- [system certificate crl](#)
- [system certificate local](#)
- [system certificate remote](#)

system certificate crl

Use this command to import certificate revocation lists.

To ensure that your FortiMail unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses. For more information, see the *FortiMail Administration Guide*.

Syntax

```
config system certificate crl
  edit <name_str>
    set crl <cert_str>
  end
```

Variable	Description	Default
<name_str>	Enter a name for this certificate revocation list.	
crl <cert_str>	Enter or paste the certificate in PEM format to import it.	

Related topics

- [system certificate ca](#)

- [system certificate local](#)
- [system certificate remote](#)

system certificate local

Use this command to import signed certificates and certificate requests in order to install them for local use by the FortiMail unit.

FortiMail units require a local server certificate that it can present when clients request secure connections, including:

- the web-based manager (HTTPS connections only)
- webmail (HTTPS connections only)
- secure email, such as SMTPS, IMAPS, and POP3S



When using this command to import a local certificate, you must enter the commands in the order described in the following syntax. This is because the "set privatekey...." will need the password to decrypt the private key if it was encrypted and "set certificate" will try to find a matched private key file.

Syntax

```
config system certificate local
    edit <name_str>
        set password
        set private-key
        set certificate <cert_str>
        set csr <csr_str>
        set comments <comment_str>
    end
```

Variable	Description	Default
<name_str>	Enter a name for the certificate to be imported.	
password	Enter a password for the certificate.	
private-key	Enter a private key for the certificate.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	
csr <csr_str>	Enter or paste the certificate signing request in PEM format to import it.	
comments <comment_str>	Enter any comments for this certificate.	

Related topics

- [system certificate ca](#)
- [system certificate crt](#)
- [system certificate remote](#)

system certificate remote

Use this command to import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA).

OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).

Remote certificates are required if you enable OCSP for PKI users.

Syntax

```
config system certificate remote
  edit <name_str>
    set certificate <cert_str>
  end
```

Variable	Description	Default
<name_str>	Enter a name for the certificate to be imported.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	

Related topics

- [system certificate ca](#)
- [system certificate crl](#)
- [system certificate local](#)

system ddns

Use this command to configure the FortiMail unit to update a dynamic DNS (DDNS) service with its current public IP address.

Syntax

```
config system ddns
  edit <ddns-service_str>
    config domain
      edit domain <domain_str>\
        set ipmode {auto | bind | static}
        set interface <interface_str>
        set ip <host_ipv4>
        set status {enable | disable}
        set type {custom | dynamic | static}
      set password <password_str>
      set timeout <time_int>
      set username <username_str>
    end
```

Variable	Description	Default
<code><ddns-service_str></code>	<p>Enter one of the following DDNS update servers:</p> <ul style="list-style-type: none"> members.dhs.org dipdnsserver.dipdns.com www.dnsart.com members.dyndns.org www.dyns.net ip.todayisp.com ods.org rh.tzo.com ph001.oray.net <p>Note: You must have an account with this DDNS service provider.</p>	
<code>domain</code> <code><domain_str></code>	Enter the domain name that is tied to this username and server.	
<code>ipmode {auto bind static}</code>	<p>Select the method of determining the IP address:</p> <ul style="list-style-type: none"> <code>auto</code>: Automatically detect the public IP address of the FortiMail unit and use that as the IP address to which <code>domain <domain_str></code> will resolve. <code>bind</code>: Use the IP address of a specific network interface as the IP address to which <code>domain <domain_str></code> will resolve. Also configure <code>interface <interface_str></code>. <code>static</code>: Use the public IP address to which <code>domain <domain_str></code> will resolve. Also configure <code>ip <host_ipv4></code>. 	auto
<code>interface</code> <code><interface_str></code>	Enter the specific network interface of which the IP address is used as the IP address to which <code>domain <domain_str></code> will resolve.	
<code>ip <host_ipv4></code>	Enter the public IP address to which <code>domain <domain_str></code> will resolve.	
<code>status {enable disable}</code>	Enable to notify a DDNS service provider to update public DNS records when the public IP address of the FortiMail unit changes.	disable
<code>type {custom dynamic static}</code>	Enter a service type for this domain.	
<code>password</code> <code><password_str></code>	Enter the password of the DDNS account.	
<code>timeout</code> <code><time_int></code>	Enter the amount of time in hours after which your FortiMail unit will contact the DDNS server to reaffirm its current IP address.	
<code>username</code> <code><username_str></code>	Enter the user name of your account with the DDNS service provider.	

Related topics

- [system dns](#)

system disclaimer

Use this command to configure system-wide disclaimer messages.

A disclaimer message is text that is generally attached to email to warn the recipient that the email contents may be confidential. For disclaimers added to outgoing messages, you need to configure an IP-based policy or an outgoing recipient-based policy.

Disclaimer messages can be appended for either or both incoming or outgoing email messages. For information on determining the directionality of an email message, see the *FortiMail Administration Guide*.

Syntax

```
config system disclaimer
    set exclude-status {enable | disable}
    set incoming-body-content <disclaimer_str>
    set incoming-body-content-html
    set incoming-body-status {enable | disable}
    set incoming-header-insertion-name
    set incoming-header-insertion-value
    set incoming-header-content <disclaimer_str>
    set incoming-header-status {enable | disable}
    set outgoing-body-content <disclaimer_str>
    set outgoing-body-content-html
    set outgoing-body-location
    set outgoing-body-status {enable | disable}
    set outgoing-header-content <disclaimer_str>
    set outgoing-header-status {enable | disable}
end
```

Variable	Description	Default
exclude-status {enable disable }	If you do not want to insert disclaimers to the email messages from certain senders or to certain recipients, you can enable this option. For information about how to configure the disclaimer exclusion list, see “ system disclaimer-exclude ” on page 261.	disable
incoming-body-content <disclaimer_str>	Enter the text that comprises the disclaimer message that appends to the message body of each incoming email.	
incoming-body-content-html	Enter the text that comprises the content of the html incoming disclaimer in the message body.	
incoming-body-status {enable disable }	Enable to append a disclaimer to the message body of each incoming email. Also configure incoming-body-content <disclaimer_str> .	disable

Variable	Description	Default
incoming-header-insertion-name	Enter the name of the header to be inserted for incoming disclaimer.	
incoming-header-insertion-value	Enter the balue of the header to be inserted for incoming disclaimer.	
incoming-header-content <disclaimer_str>	Enter the text that comprises the disclaimer message that is inserted into the message header of each incoming email.	
incoming-header-status {enable disable }	Enable to insert a disclaimer to the message header of each incoming email. Also configure incoming-header-content <disclaimer_str> .	disable
outgoing-body-content <disclaimer_str>	Enter the text that comprises the disclaimer message that appends to the message body of each outgoing email.	
outgoing-body-content-html	Enter the content of html outgoing disclaimer in the message body.	
outgoing-body-location	Enter the outgoing disclaimer at the beginning or ending of the message body.	
outgoing-body-status {enable disable }	Enable to append a disclaimer to the message body of each outgoing email. Also configure outgoing-body-content <disclaimer_str> .	disable
outgoing-header-content <disclaimer_str>	Enter the text that comprises the disclaimer message that is inserted into the message header of each outgoing email.	
outgoing-header-status {enable disable }	Enable to insert a disclaimer to the message header of each outgoing email. Also configure outgoing-body-content <disclaimer_str> .	disable

Related topics

- [system disclaimer-exclude](#)

system disclaimer-exclude

In some cases, you may not want to insert disclaimers to some email messages. For example, you may not want to insert disclaimers to paging text or SMS text messages. To do this, you add the specific senders, sender domains, recipients, or recipients domains to the exclusion list, and when you configure the global disclaimer settings (see [“system disclaimer” on page 260](#), you can enable the exclusion list.

Syntax

```
config system disclaimer-exclude
edit <id>
    set recipient-pattern <string>
    set sender-pattern <string>
end
```

Variable	Description	Default
<id>	Enter a table ID.	
recipient-pattern <string>	Enter a recipient pattern. For example, if you add *@example.com, all messages to example.com users will be exempted from disclaimer insertion	
sender-pattern <string>	Enter a sender pattern. For example, if you add *@example.com, all messages from example.com users will be exempted from disclaimer insertion	

Related topics

- [system disclaimer](#)

system dns

Use this command to configure the IP addresses of the primary and secondary DNS servers that the FortiMail unit will query to resolve domain names into IP addresses.

Starting from v5.0.2 release, you can also configure up to 3 other DNS servers for protected domains' (and their domain associations) MX record query only. This is useful if the protected domains' MX record or A record are resolved differently on internal DNS servers. This feature is only applicable to gateway mode and transparent mode and when you select MX record as the relay type in domain settings. Note that if you configure DNS servers for protected domains (such as example.com), FortiMail will also use the same DNS server for all queries that are in the form of anysub.example.com, so that the recursive queries for the returned MX record (mx.example.com) or other records can be directed the the same server.

Syntax

```
config system dns
    set cache {enable | disable}
    set primary <ipv4_address>
    set private_ip_query {enable | disable}
    set protected-domain-dns-servers <ipv4_address>
    set protected-domain-dns-state {enable | disable}
    set secondary <dns_ipv4>
    set truncate-handling {disable | tcp-retry}
end
```

Variable	Description	Default
cache {enable disable }	Enable to cache DNS query results to improve performance. Disable the DNS cache to free memory if you are low on memory.	enable
primary <ipv4_address>	Enter the IP address of the primary DNS server.	0.0.0.0

Variable	Description	Default
private_ip_query {enable disable }	Enable to perform reverse DNS lookups on private network IP addresses, as defined in RFC 1918. The DNS server must have PTR records for your private network's IP addresses. Failure to contain records for those IP addresses may increase DNS query time and cause query results to be 'Host not found'.	disable
protected-domain-dns-servers <ipv4_address>	Enter the IP address of the DNS servers that you want to use to resolve the protected domain names (including their subdomains). You can enter up to 3 addresses/DNS servers.	0.0.0.0
protected-domain-dns-state {enable disable}	Either enable or disable the protected domain DNS servers.	disable
secondary <dns_ipv4>	Enter the IP address of the secondary DNS serve.	0.0.0.0
truncate-handling {disable tcp-retry}	Specify how to handle truncated UDP replies of DNS queries: select either disable (meaning no retries) or tcp-try (meaning retry in TCP mode).	tcp-retry

Related topics

- [system ddns](#)

system encryption ibe

Use this command to configure, enable, or disable Identity-Based Encryption (IBE) services, which control how secured mail recipients use the FortiMail IBE function.

Syntax

```

config system encryption ibe
    set custom-user-control-status {enable | disable}
    set expire-emails <days_int>
    set expire-inactivity <days_int>
    set expire-passwd-reset <hours_int>
    set expire-registration <days_int>
    set read-notification {enable | disable}
    set secure-compose {enable | disable}
    set secure-reply {enable | disable}
    set secure-forward {enable | disable}
    set service-name <name_str>
    set status {enable | disable}
    set unread-days
    set unread-notif-rcpt
    set unread-notif-sender
    set unread-notification {enable | disable}
    set url-about <url_str>
    set url-base <url_str>
    set url-custom-user-control <url_str>
    set url-forgot-pwd <psw_str>
    set url-help <url_str>
end

```

Variable	Description	Default
custom-user-control-status {enable disable}	If your corporation has its own user authentication tools, enable this option and enter the URL. Also configure url-custom-user-control and url-forgot-pwd.	disable
expire-emails <days_int>	Enter the number of days that the secured mail will be saved on the FortiMail unit.	180
expire-inactivity <days_int>	Enter the number of days the secured mail recipient can access the FortiMail unit without registration. For example, if you set the value to 30 days and if the mail recipient did not access the FortiMail unit for 30 days after he/she registers on the unit, the recipient will need to register again if another secured mail is sent to him/her. If the recipient accessed the FortiMail unit on the 15th days, the 30-day limit will be recalculated from the 15th day onwards.	90
expire-passwd-reset <hours_int>	Enter the password reset expiry time in hours. This is for the recipients who have forgotten their login passwords and request for new ones. The secured mail recipient must reset his/her password within this time limit to access the FortiMail unit.	24
expire-registration <days_int>	Enter the number of days that the secured mail recipient has to register on the FortiMail unit to view the mail before the registration expires. The starting date is the date when the FortiMail unit sends out the first notification to a mail recipient.	30

Variable	Description	Default
read-notification {enable disable}	Enable to send the read notification the first time the mail is read.	disable
secure-compose {enable disable}	Select to allow the secure mail recipient to compose an email. The FortiMail unit will use policies and mail delivery rules to determine if this mail needs to be encrypted. For encrypted email, the domain of the composed mail's recipient must be a protected one, otherwise an error message will appear and the mail will not be delivered.	disable
secure-reply {enable disable}	Allow the secured mail recipient to reply to the email with encryption.	disable
secure-forward {enable disable}	Allow the secured mail recipient to forward the email with encryption	disable
service-name <name_str>	Enter the name for the IBE service. This is the name the secured mail recipients will see once they access the FortiMail unit to view the mail.	
status {enable disable}	Enable the IBE service you have configured.	disable
unread-days		
unread-notif-rcpt	Enable to send the unread notification to the recipient.	disable
unread-notif-sender	Enable to send the unread notification to the sender.	disable
unread-notification {enable disable}	Enable to send the unread notification if the message remains unread for 14 days by default.	disable
url-about <url_str>	You can create a file about the FortiMail IBE encryption and enter the URL for the file. The mail recipient can click the "About" link from the secure mail notification to view the file. If you leave this option empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification.	
url-base <url_str>	Enter the FortiMail unit URL, for example, https://192.168.100.20, where a mail recipient can register or authenticate to access the secured mail.	
url-custom-user-control <url_str>	Enter the URL where you can check for user existence. This command appears after you enable custom-user-control-status.	

Variable	Description	Default
url-forgot-pwd <psw_str>	Enter the URL where users get authenticated. This command appears after you enable custom-user-control-status.	
url-help <url_str>	You can create a help file on how to access the FortiMail secure email and enter the URL for the file. The mail recipient can click the “Help” link from the secure mail notification to view the file. If you leave this option empty, a default help file link will be added to the secure mail notification.	

Related topics

- [system encryption ibe-auth](#)

system encryption ibe-auth

When mail recipients of the IBE domains access the FortiMail unit after receiving a secure mail notification:

- recipients of the IBE domains without LDAP authentication profiles need to register to view the email.
- recipients of the IBE domains with LDAP authentication profiles just need to authenticate because the FortiMail unit can query the LDAP servers for authentication information based on the LDAP profile.

In both cases, the FortiMail unit will record the domain names of the recipients who register or authenticate on it under the *User > IBE User > IBE Domain* tab.

Use this command to bind domains with LDAP authentication profiles with which the FortiMail unit can query the LDAP servers for authentication, email address mappings, and more. For more information about LDAP profiles, see [“profile ldap” on page 211](#).

Syntax

```
config system encryption ibe-auth
    edit <id>
        set domain-pattern <string>
        set ldap-profile <profile_name>
        set status {enable | disable}
    end
```

Variable	Description	Default
<id>	Enter a table ID.	
domain-pattern <string>	Enter a domain name that you want to bind to an LDAP authentication profile. If you want all IBE users to authenticate through an LDAP profile and do not want other non-LDAP-authenticated users to get registered on FortiMail, you can use wildcard * for the domain name and then bind it to an LDAP profile.	

Variable	Description	Default
ldap-profile <profile_name>	Enter a profile name from the available LDAP profile list, which you want to use to authenticate the domain users.	
status {enable disable}	Enable or disable the rule.	disable

Related topics

- [system encryption ibe](#)

system fortiguard antivirus

Use this command to configure how the FortiMail unit will retrieve the most recent updates to FortiGuard Antivirus engines, antivirus definitions, and antispam definitions (the heuristic antispam rules only). FortiMail can get antivirus updates either directly from an FDN server or via a web proxy.

Syntax

```
config system fortiguard antivirus
    set override-server-address <virtual-ip_ipv4>
    set override-server-status {enable | disable}
    set push-update-override-address <virtual-ip_ipv4>
    set push-update-override-port <port_int>
    set push-update-override-status {enable | disable}
    set push-update-status {enable | disable}
    set scheduled-update-day <day_int>
    set scheduled-update-frequency {daily | every | weekly}
    set scheduled-update-status {enable | disable}
    set scheduled-update-time <time_str>
    set tunneling-address <host_ipv4>
    set tunneling-password <password_str>
    set tunneling-port <port_int>
    set tunneling-status {enable | disable}
    set tunneling-username <username_str>
    set virus-db
    set virus-outbreak
    set virus-outbreak-protection-period
end
```

Variable	Description	Default
override-server-address <virtual-ip_ipv4>	If override-server-status is enable, enter the IP address of the public or private FortiGuard Distribution Server (FDS) that overrides the default FDS to which the FortiMail unit connects for updates.	
override-server-status {enable disable}	Enable to override the default FDS to which the FortiMail unit connects for updates.	disable

Variable	Description	Default
push-update-override-address <virtual-ip_ipv4>	If push-update-override-status is enable, enter the public IP address that will forward push updates to the FortiMail unit. Usually, this is a virtual IP address on the external interface of a NAT device such as a firewall or router.	
push-update-override-port <port_int>	If push-update-override-status is enable, enter the port number that will forward push updates to UDP port 9443 the FortiMail unit. Usually, this is a port forward on the external interface of a NAT device such as a firewall or router.	
push-update-override-status {enable disable}	Enable to override the default IP.	disable
push-update-status {enable disable}	Enable to allow the FortiMail unit to receive notifications of available updates, which trigger it to download FortiGuard Antivirus packages from the Fortinet Distribution Network (FDN).	disable
scheduled-update-day <day_int>	Enter the day of the week at which the FortiMail unit will request updates where the range is from 0-6 and 0 means Sunday and 6 means Saturday.	
scheduled-update-frequency {daily every weekly}	Enter the frequency at which the FortiMail unit will request updates. Also configure scheduled-update-day <day_int> and scheduled-update-time <time_str>.	weekly
scheduled-update-status {enable disable}	Enable to perform updates according to a schedule.	enable
scheduled-update-time <time_str>	Enter the time of the day at which the FortiMail unit will request updates, in the format hh:mm, where hh is the number of hours and mm is the number of minutes after the hour in 15 minute intervals.	01:00
tunneling-address <host_ipv4>	If tunneling-status is enable, enter the IP address of the web proxy.	
tunneling-password <password_str>	If tunneling-status is enable, enter the password of the account on the web proxy.	
tunneling-port <port_int>	If tunneling-status is enable, enter the TCP port number on which the web proxy listens.	
tunneling-status {enable disable}	Enable to tunnel update requests through a web proxy.	disable
tunneling-username <username_str>	If tunneling-status is enable, enter the user name of the FortiMail unit's account on the web proxy.	
virus-db		disable
virus-outbreak		disable
virus-outbreak-protection-period		disable

Related topics

- [system fortiguard antispam](#)
- [update](#)
- [debug application updated](#)

system fortiguard antispam

Use this command to configure how the FortiMail unit will connect to the FortiGuard servers to query for antispam signatures. Unlike the antivirus updates, FortiMail cannot query FortiGuard antispam service via a web proxy. If there is a web proxy before FortiMail, you have to use a FortiManager unit locally as an override server.

Syntax

```
config system fortiguard antispam
    set cache-mpercent <percentage_int>
    set cache-status {enable | disable}
    set cache ttl <ttl_int>
    set hostname {<fqdn_str> | <host_ipv4>}
    set outbreak-protection-level {disable | highg | low | medium}
    set outbreak-protecdtion-period <minutes>
    set port {53 | 8888 | 8889}
    set query-timeout <timeout_int>
    set server-override-ip <ipv4>
    set server-override-status {enable | disable}
    set status {enable | disable}
    set uri-redirect-lookup {enable | disable}
end
```

Variable	Description	Default
cache-mpercent <percentage_int>	Enter the percentage of memory the antispam cache is allowed to use in percentage. The range is 1-15%.	2
cache-status {enable disable }	Enable cache and specify the cache TTL time to improve performance.	enable
cache ttl <ttl_int>	Enter the time to live (TTL) in seconds for cache entries.	300
hostname {<fqdn_str> <host_ipv4>}	Enter an IP address or a fully qualified domain name (FQDN) to override the default FortiGuard Antispam query server.	antispam .fortiga te.com

Variable	Description	Default
outbreak-protection-level {disable high low medium}	Specify a spam outbreak protection level. Higher level means more strict filtering. This feature temporarily hold email for a certain period of time (configurable with the CLI command <code>outbreak-protection-period</code>) if the enabled FortiGuard antispam check (black IP and/or URI filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs.	low
outbreak-protection-period <minutes>	Specify how long (in minutes) FortiMail will hold email before it query the FortiGuard server for the second time.	30
port {53 8888 8889}	Enter the port number used to communicate with the FortiGuard Antispam query servers.	53
query-timeout <timeout_int>	Enter the timeout value for the FortiMail unit to query the FortiGuard Antispam query server.	7
server-override-ip <ipv4>	If <code>server-override-status</code> is enable, enter the IP address of the public or private FortiGuard Antispam query server that overrides the default query server to which the FortiMail unit connects.	
server-override-status {enable disable }	Enable to override the default FortiGuard Antispam query server to which the FortiMail unit connects to and checks for antispam signatures.	disable
status {enable disable }	Enable to query to the FortiGuard Distribution Network (FDN) for FortiGuard Antispam ratings. This option must be enabled for antispam profiles where the FortiGuard Antispam scan is enabled to have an effect.	enable
uri-redirect-lookup {enable disable }	If an email contains a shortened URI that redirects to another URI, the FortiMail unit is able to send a request to the shortened URI to get the redirected URI and scan it against the FortiGuard AntiSpam database. By default, this function is enabled. To use it, you need to open your HTTP port to allow the FortiMail unit to send request for scanning the redirected URI.	enable

Related topics

- [system fortiguard antivirus](#)
- [update](#)
- [debug application updated](#)

system fortisandbox

The FortiSandbox unit is used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus

profiles. If the file exhibits risky behavior, or is found to contain a virus, the result will be sent back to FortiMail and a new virus signature is created and added to the FortiGuard antivirus signature database. For more information about FortiSandbox, please visit Fortinet's web site at <http://www.fortinet.com>.

Syntax

```
config system fortisandbox
  config file-pattern
    edit <table_value>
      set pattern <string>
    end
  config file-types
    edit {adobe-flash | archive | html | jar | javascript | pdf |
      msoffice-document | windows-exectuable}
      set status {enable | disable}
    end
  set admin-email <email_str>
  set host <hostname_or_ip>
  set max-file-size <integer_value>
  set max-file-size-status {enable | disable}
  set max-uri-per-email
  set max-uri-per-email
  set scan-exception-as {clean | malicious | high-risk | medium-risk
    | low-risk}
  set scan-mode {scan-and-wait | scan-only}
  set scan-order {antispam-content-sandbox |
    antispam-sandbox-content | sandbox-antispam-content}
  set set scan-result-retention
  set scan-timeout
  set service-type
  set statistics-interval <1-30-minutes>
  set status {enable | disable}
  set uri-scan-category
  set uri-scan-email-selection
  set uri-scan-on-rating-error {enable | disable}
end
```

Variable	Description	Default
file-pattern	Enter the file patterns to upload to FortiSandbox	
<table_value>	Enter the item number to edit.	
pattern <string>	Enter the pattern value.	
file-types	Enter the file types to upload to FortiSandboxfor scanning.	
edit <file_types>	Enter the desired attachment type to include in FortiSandbox's scanning.	
status {enable disable}	Enable or disable the selected file type from FortiSanbox's scanning.	

Variable	Description	Default
admin-email <email_str>	Enter the administrator's email address to receive reports and notifications.	
max-file-size <integer_value>	Enter the maximum size in kilobytes for files uploaded to FortiSandbox.	
max-file-size-status {enable disable}	Enable or disable the maximum size for files uploaded to FortiSandbox.	
host <hostname_or_ip>	Enter the host name or IP address of the FortiSandbox.	
max-uri-per-email	Maximum number of uris per email to be scanned. Range between 5-20.	5
scan-exception-as {clean malicious high-risk medium-risk low-risk}	Specify different actions to take when FortiSandbox returns a scan exception. The corresponding actions are listed under the FortiSandbox settings in the antivirus profiles.	clean
scan-mode {scan-and-wait scan-only}	scan-and-wait means to submit the suspicious email to FortiSandbox and wait for the results. scan-only means just to submit the suspicious email without waiting for the results.	scan-and-wait
scan-order {antispam-content-sandbox antispam-sandbox-content sandbox-antispam-content}	Set the order of scanners. Sending files to FortiSandbox usually takes more bandwidth and thus it is better to use it as the last resort.	antispam-content-sandbox
scan-result-retention	Scan result retention period in minutes.	60
scan-timeout	Timeout value before discarding unfinished scan tasks.	30
service-type	Use FortiSandbox appliance or FortiSandbox cloud service.	
statistics-interval <1-30-minutes>	Specify how long FortiMail should wait to retrieve some high level statistics from FortiSandbox. The statistics include how many malwares are detected and how many files are clean among all the files submitted	5
status {enable disable}	Either enable or disable the usage of the unit.	disable
uri-scan-category	Category of the uri to be scanned.	
uri-scan-email-selection	Selection of email for uri scan.	
uri-scan-on-rating-error {enable disable}	Sometimes, FortiMail may not be able to get results from the FortiGuard queries (for example, ratings errors due to network connection failures). In this case, you can choose whether to upload the those URIs to FortiSandbox for scanning. Choosing not to upload those URIs may help improving the FortiSandbox performance.	disable

system global

Use this command to configure many FortiMail system-wide configurations.

Syntax

```
config system global
  set admin-idle-timeout <timeout_int>
  set admin-scp {enable | disable}
  set default-certificate <name_str>
  set dh-params <params_int>
  set disclaimer-per-domain {enable | disable}
  set disk-monitor {enable | disable}
  set hostname <host_str>
  set iscsi-initiator-name <name_str>
  set lcd-pin <pin_int>
  set lcd-protection {enable | disable}
  set ldap-server-sys-status {enable | disable}
  set ldap-sess-cache-state {enable | disable}
  set local-domain-name <name_str>
  set mta-adv-ctrl-status {enable | disable}
  set operation mode {gateway | server | transparent}
  set pki-certificate-req {yes | no}
  set pki-mode {enable | disable}
  set port-http <port_int>
  set port-https <port_int>
  set port-ssh <port_int>
  set port-telnet <port_int>
  set post-login-banner {admin | ibe | webmail}
  set pre-login-banner admin
  set rest-api
  set ssl-versions {ssl3 | tls1_0 | tls1_1 | tls1_2}
  set strong-crypto {enable | disable | enable-mail-rc4}
  set tftp {enable | disable}
end
```

Variable	Description	Default
admin-idle-timeout <timeout_int>	Enter the amount of time in minutes after which an idle administrative session will be automatically logged out. The maximum idle time out is 480 minutes (8 hours). To improve security, do not increase the idle timeout.	5
admin-scp {enable disable}	Enable to allow system configuration download by SCP.	disable
default-certificate <name_str>	Enter the name of a local certificate to use it as the "default" (that is, currently chosen for use) certificate. FortiMail units require a local server certificate that it can present when clients request secure connections.	factory

Variable	Description	Default
dh-params <params_int>	Enter the minimum size of Diffie-Hellman prime for SSH/HTTPS.	1024
disclaimer-per-domain {enable disable}	Enable to allow individualized disclaimers to be configured for each protected domain.	
disk-monitor {enable disable}	Enable to monitor the hard disk status of the FortiMail unit. If a problem is found, an alert email is sent to the administrator.	disable
hostname <host_str>	Enter the host name of the FortiMail unit.	Varies by model.
iscsi-initiator-name <name_str>	Enter the FortiMail iSCSI client name used to communicate with the iSCSI server for centralized quarantine storage. This is only used to change the name generated by the FortiMail unit automatically.	
lcd-pin <pin_int>	Enter the 6-digit personal identification number (PIN) that administrators must enter in order to access the FortiMail LCD panel. The PIN is used only when <code>lcdprotection</code> is <code>enable</code> .	Encoded value varies.
lcd-protection {enable disable}	Enable to require that administrators enter a PIN in order to use the buttons on the front LCD panel. Also configure <code>lcdpin</code> .	disable
ldap-server-status {enable disable}	Enable/disable the LDAP server for serving organizational information.	enable
ldap-sess-cache-state {enable disable}	Enable to keep the continuity of the connection sessions to the LDAP server. Repeated session connections waste network resources.	enable
local-domain-name <name_str>	Enter the local domain name of the FortiMail unit.	
mta-adv-ctrl-status {enable disable}	Enable to configure session-specific MTA settings and overwrite the global settings configured elsewhere.	enable
operation mode {gateway server transparent}	Enter one of the following operation modes: <ul style="list-style-type: none"> <code>gateway</code>: The FortiMail unit acts as an email gateway or MTA, but does not host email accounts. <code>server</code>: The FortiMail unit acts as a standalone email server that hosts email accounts and acts as an MTA. <code>transparent</code>: The FortiMail unit acts as an email proxy. 	gateway

Variable	Description	Default
pki-certificate-req {yes no}	If the administrator's web browser does not provide a valid personal certificate for PKI authentication, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter <code>yes</code> . To allow password-style fallback, enter <code>no</code> .	no
pki-mode {enable disable}	Enable to allow PKI authentication for FortiMail administrators. For more information, see "user pki" on page 313 and "system admin" on page 249 . Also configure <code>pki-certificate-req {yes no}</code> . Caution: Before disabling PKI authentication, select another mode of authentication for FortiMail administrators and email users that are currently using PKI authentication. Failure to first select another authentication method before disabling PKI authentication will prevent them from being able to log in.	disable
port-http <port_int>	Enter the HTTP port number for administrative access on all interfaces.	80
port-https <port_int>	Enter the HTTPS port number for administrative access on all interfaces.	443
port-ssh <port_int>	Enter the SSH port number for administrative access on all interfaces.	22
port-telnet <port_int>	Enter the TELNET port number for administrative access on all interfaces.	23
post-login-banner {admin ibe webmail}	Enable or disable the legal disclaimer. <ul style="list-style-type: none"> <code>admin</code>: Select to display the disclaimer message after the administrator logs into the FortiMail web UI. <code>webmail</code>: Select to display the disclaimer message after the user logs into the FortiMail webmail. <code>ibe</code>: Select to display the disclaimer message after the user logs into the FortiMail unit to view IBE encrypted email. 	admin
pre-login-banner admin	Enable or disable the legal disclaimer before the administrator logs into the FortiMail web UI.	admin
rest-api	Enable or disable ssl protocol versions	disable
ssl-versions {ssl3 tls1_0 tls1_1 tls1_2}	Specify which SSL/TLS versions you want to support for the HTTPS access to FortiMail. Currently, SSL 3, TLS 1.0, TLS 1.1, and TLS 1.2 are supported.	ssl3, tls1_0, tls1_1, tls1_2

Variable	Description	Default
strong-crypto {enable disable enable-mail-rc4}	<p>Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access.</p> <p>When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta) and higher.</p> <p>Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.</p> <p>Enable the mail RC4 option to force the SMTP service to use the RC4-SHA ciphers.</p>	disable
tftp {enable disable }	Enable to allow use of TFTP in FIPS mode.	enable

Related topics

- [config domain-setting](#)

system ha

Use this command to configure the FortiMail unit to act as a member of a high availability (HA) cluster in order to increase processing capacity or availability. It also enables you to monitor the HA cluster.

Syntax

```
config system ha
  config interface
    edit <interface_name>
      set action-on-master {ignore-vip | use-vip}
      set heartbeat-status <disable | primary | secondary>
      set peer-ip <ipv4_netmask>
      set peer-ip6 <ipv6_netmask>
      set port-monitor {enable | disable}
      set virtual-ip <ipv4_netmask>
      set virtual-ip6 <ipv6_netmask>
  config service
    edit <remote-smtp>
      set check-interval <integer>
      set check-timeout <integer>
      set ip <ip_addr>
      set port <port_num>
      set retries <integer>
      set status {enable | disable}
    edit <remote-imap>
      set check-interval <integer>
      set check-timeout <integer>
      set ip <ip_addr>
      set port <port_num>
      set retries <integer>
      set status {enable | disable}
    edit <remote-pop>
      set check-interval <integer>
      set check-timeout <integer>
      set ip <ip_addr>
      set port <port_num>
      set retries <integer>
      set status {enable | disable}
    edit <remote-http>
      set check-interval <integer>
      set check-timeout <integer>
      set ip <ip_addr>
      set port <port_num>
      set retries <integer>
      set status {enable | disable}
    edit <local-ports>
      set check-interval <integer>
      set retries <integer>
      set status {enable | disable}
    edit <local-hd>
      set check-interval <integer>
      set retries <integer>
      set status {enable | disable}
```

```

set config-peer-ip <ip_addr>
set hb-base-port <interface_int>
set hb-lost-threshold
set heartbeat-1-interface <interface_int>
set heartbeat-1-ip <local_ipv4mask>
set heartbeat-1-peer <primary-peer_ipv4>
set heartbeat-2-interface <interface_str>
set heartbeat-2-ip <secondary-local_ipv4mask>
set heartbeat-2-peer <secondary-peer_ipv4>
set mail-data-sync {enable | disable}
set mailqueue-data-sync {enable | disable}
set mode {config-master | config-slave | master | off | slave}
set on-failure {off | restore-role | become-slave}
set password <password_str>
set remote-services-as-heartbeat {enable | disable}
end

```

Variable	Description	Default
<interface_name>	Enter the interface name of which you want to configure the virtual IP.	
action-on-master {ignore-vip use-vip}	<p>Select whether and how to configure the IP addresses and netmasks of the FortiMail unit whose effective HA mode of operation is currently master.</p> <ul style="list-style-type: none"> ignore-vip: Do not change the network interface configuration on failover, and do not monitor. use-vip: Add the specified virtual IP address and netmask to the network interface on failover. Normally, you will configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. Both originating and reply traffic uses the virtual IP address. This option results in the network interface having two IP Addresses: the actual and the virtual. 	ignore-v ip

Variable	Description	Default
heartbeat-status <disable primary secondary>	<p>Specify if this interface will be used for HA heartbeat and synchronization.</p> <ul style="list-style-type: none"> • Disable <p>Do not use this interface for HA heartbeat and synchronization.</p> <ul style="list-style-type: none"> • Primary <p>Select the primary network interface for heartbeat and synchronization traffic.</p> <p>This network interface must be connected directly or through a switch to the <i>Primary heartbeat</i> network interface of other members in the HA group.</p> <ul style="list-style-type: none"> • Secondary <p>Select the secondary network interface for heartbeat and synchronization traffic.</p> <p>The secondary heartbeat interface is the backup heartbeat link between the units in the HA group. If the primary heartbeat link is functioning, the secondary heartbeat link is used for the HA heartbeat. If the primary heartbeat link fails, the secondary link is used for the HA heartbeat and for HA synchronization.</p> <p>This network interface must be connected directly or through a switch to the <i>Secondary heartbeat</i> network interfaces of other members in the HA group.</p> <p>Caution: Using the same network interface for both HA synchronization/heartbeat traffic and other network traffic could result in issues with heartbeat and synchronization during times of high traffic load, and is not recommended.</p> <p>Note: In general, you should isolate the network interfaces that are used for heartbeat traffic from your overall network. Heartbeat and synchronization packets contain sensitive configuration information, are latency-sensitive, and can consume considerable network bandwidth.</p>	
peer-ip <ipv4_netmask>	<p>Enter the IP address of the matching heartbeat network interface of the other member of the HA group.</p> <p>For example, if you are configuring the primary unit's primary heartbeat network interface, enter the IP address of the secondary unit's primary heartbeat network interface.</p> <p>Similarly, for the secondary heartbeat network interface, enter the IP address of the other unit's secondary heartbeat network interface.</p> <p>This option appears only for active-passive HA.</p>	
peer-ip6 <ipv6_netmask>	<p>Enter the peer IPv6 address in the active-passive HA group.</p>	

Variable	Description	Default
port-monitor {enable disable }	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover. This option applies only if local network interface monitoring is enabled.	
virtual-ip <ipv4_netmask>	Enter the virtual IP address and netmask for this interface. This option is available only if <code>action-on-master {ignore-vip use-vip}</code> is set.	0.0.0.0/ 0
virtual-ip6 <ipv6_netmask>	Enter the virtual IPv6 address and netmask for this interface. This option is available only if <code>action-on-master {ignore-vip use-vip}</code> is set.	0.0.0.0/ 0
<remote-smtp>	Enter to configure the remote SMTP service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
check-timeout <integer>	Enter the timeout for remote service check in seconds.	30
ip <ip_addr>	Enter the SMTP server IP address for service check.	0.0.0.0
port <port_num>	Enter the SMTP server port number for service check.	25
retries <integer>	Enter the number of attempts to try before considering the SMTP server a failure.	3
status {enable disable }	Enable to start the remote SMTP service monitoring.	disable
<remote-imap>	Enter to configure the remote IMAP service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
check-timeout <integer>	Enter the timeout for remote service check in seconds.	30
ip <ip_addr>	Enter the IMAP server IP address for service check.	0.0.0.0
port <port_num>	Enter the IMAP server port number for service check.	143
retries <integer>	Enter the number of attempts to try before considering the IMAP server a failure.	3
status {enable disable }	Enable to start the remote IMAP service monitoring.	disable
<remote-pop>	Enter to configure the remote POP service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
check-timeout <integer>	Enter the timeout for remote service check in seconds.	30
ip <ip_addr>	Enter the POP server IP address for service check.	0.0.0.0
port <port_num>	Enter the POP server port number for service check.	110
retries <integer>	Enter the number of attempts to try before considering the POP server a failure.	3

Variable	Description	Default
status {enable disable }	Enable to start the remote POP service monitoring.	disable
<remote-http>	Enter to configure the remote HTTP service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
check-timeout <integer>	Enter the timeout for remote service check in seconds.	30
ip <ip_addr>	Enter the HTTP server IP address for service check.	0.0.0.0
port <port_num>	Enter the HTTP server port number for service check.	80
retries <integer>	Enter the number of attempts to try before considering the HTTP server a failure.	3
status {enable disable }	Enable to start the remote HTTP service monitoring.	disable
<local-ports>	Enter to configure the local network interfaces service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
retries <integer>	Enter the number of attempts to try before considering the local network interface a failure.	3
status {enable disable }	Enable to start the local network interface service monitoring.	disable
<local-hd>	Enter to configure the local hard drives service monitoring.	
check-interval <integer>	Enter the time interval between service checks in seconds.	120
retries <integer>	Enter the number of attempts to try before considering the hard drive a failure.	3
status {enable disable }	Enable to start the local hard drive service monitoring.	disable
config-peer-ip <ip_addr>	Enter the IP address of the slave FortiMail unit.	0.0.0.0
hb-base-port <interface_int>	<p>Enter the first of four total TCP port numbers that will be used for:</p> <ul style="list-style-type: none"> the heartbeat signal synchronization control data synchronization configuration synchronization <p>Note: For active-passive groups, in addition to configuring the heartbeat, you can configure service monitoring.</p>	20000

Variable	Description	Default
hb-lost-threshold	<p>Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the backup unit assumes the role of the primary unit.</p> <p>The heartbeat will continue to check for availability once per second. To prevent premature failover when the primary unit is simply experiencing very heavy load, configure a total threshold of three (3) seconds or more to allow the backup unit enough time to confirm unresponsiveness by sending additional heartbeat signals.</p> <p>This option appears only for active-passive groups.</p> <p>Note: If the failure detection time is too short, the backup unit may falsely detect a failure when during periods of high load.</p> <p>Caution: If the failure detection time is too long the primary unit could fail and a delay in detecting the failure could mean that email is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover.</p>	15
heartbeat-1-interface <interface_int>	Enter the name of the network interface that will be used for the primary heartbeat, and that is connected directly or through a switch to the primary heartbeat interface of the other FortiMail unit(s) in the HA group.	Varies by model. (The network interface with the highest number.)
heartbeat-1-ip <local_ipv4mask>	<p>Enter the IP address and netmask of the primary network interface, separated by a space.</p> <p>Use this IP address as the value of the peer IP address when configuring <code>heartbeat-1-peer <primary-peer_ipv4></code> for the other FortiMail units in the HA group.</p>	10.0.0.1 255.255. 255.0
heartbeat-1-peer <primary-peer_ipv4>	<p>Enter the IP address of the primary heartbeat network interface on the other FortiMail unit in the HA group.</p> <p>For example, if the primary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.1, enter 10.0.0.1.</p>	10.0.0.2
heartbeat-2-interface <interface_str>	Enter the name of a network interface: Use this network interface as the secondary heartbeat network interface. It must be connected to the secondary heartbeat network interface on the other FortiMail unit in the HA group. Also configure <code>heartbeat-2-ip <secondary-local_ipv4mask></code> .	Varies by model. (The network interface with the highest number.)

Variable	Description	Default
heartbeat-2-ip <secondary-local_ipv4mask>	<p>Enter the IP address and netmask of the secondary network interface, separated by a space.</p> <p>Use this IP address as the value of the peer IP address when configuring heartbeat-2-peer <secondary-peer_ipv4> for the other FortiMail units in the HA group.</p>	0.0.0.0 0.0.0.0
heartbeat-2-peer <secondary-peer_ipv4>	<p>Enter the IP address of the secondary heartbeat network interface on the other FortiMail unit in the HA group.</p> <p>For example, if the secondary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.3, enter 10.0.0.3.</p>	0.0.0.0
mail-data-sync {enable disable }	<p>Enable to synchronize system quarantine, email archives, email users' mailboxes (server mode only), preferences, and per-recipient quarantines.</p> <p>Unless the HA cluster stores its mail data on a NAS server, you should configure the HA cluster to synchronize mail directories.</p> <p>This option applies only for active-passive groups.</p>	enable
mailqueue-data-sync {enable disable }	<p>Enable to synchronize the mail queue of the FortiMail unit.</p> <p>This option applies only for active-passive groups.</p> <p>Caution: If the primary unit experiences a hardware failure and you cannot restart it, if this option is disabled, MTA spool directory data could be lost.</p> <p>Note: Enabling this option is not recommended. Periodic synchronization can be processor and bandwidth-intensive. Additionally, because the content of the MTA spool directories is very dynamic, periodically synchronizing MTA spool directories between FortiMail units may not guarantee against loss of all email in those directories. Even if MTA spool directory synchronization is disabled, after a failover, a separate synchronization mechanism may successfully prevent loss of MTA spool data.</p>	disable

Variable	Description	Default
mode {config-master config-slave master off slave}	<p>Enter one of the following HA operating modes:</p> <ul style="list-style-type: none"> <code>config-master</code>: Enable HA and operate as the primary unit in a config-only HA group. <code>config-slave</code>: Enable HA and operate as the backup unit in a config-only HA group. <code>master</code>: Enable HA and operate as the primary unit in an active-passive HA group. <code>off</code>: Disable HA. Each FortiMail unit operates independently. <code>slave</code>: Enable HA and operate as the backup unit in an active-passive HA group. <p>Caution: For config-only HA, if the FortiMail unit is operating in server mode, you must store mail data externally, on a NAS server. Failure to store mail data externally could result in mailboxes and other data scattered over multiple FortiMail units. For details on configuring NAS, see the FortiMail Administration Guide.</p>	off
on-failure {off restore-ro le become-slave}	<p>Enter one of the following behaviors of the primary unit when it detects a failure.</p> <ul style="list-style-type: none"> <code>off</code>: Do not process email or join the HA group until you manually select the effective operating mode. <code>restore-role</code>: On recovery, the failed primary unit's effective operating mode resumes its configured operating mode. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent. <code>become-slave</code>: On recovery, the failed primary unit's effective operating mode becomes SLAVE (backup), and it then synchronizes the content of its MTA spool directories with the current primary unit. The new primary unit can then deliver email that existed in the former primary unit's MTA spool at the time of the failover. <p>In most cases, you should enter <code>become-slave</code>.</p> <p>For details on the effects of this option on the effective operating mode, see the FortiMail Administration Guide. This option applies only if the FortiMail unit is operating in an active-passive HA group, as a primary unit.</p>	
password <password_str>	Enter a password for the HA group. The password must be the same on the primary and backup FortiMail unit(s). The password must be a least 1 character.	change_me
remote-services-as-heartbeat {enable disable }	<p>Enable to use remote service monitoring as a tertiary heartbeat signal.</p> <p>This option applies only for FortiMail units operating in the active-passive HA mode, and requires that you also configure remote service monitoring using.</p>	

Related topics

- [system global](#)
- [debug application hahbd](#)
- [debug application hasyncd](#)
- [system ha](#)

system interface

Use this command to configure allowed and denied administrative access protocols, maximum transportation unit (MTU) size, SMTP proxy, and up or down administrative status for the network interfaces of a FortiMail unit.

Proxy and built-in MTA behaviors are configured separately based upon whether the SMTP connection is considered to be incoming or outgoing. Because a network connection considers the network layer rather than the application layer when deciding whether to intercept a connection, the concept of incoming and outgoing connections is based upon slightly different things than that of incoming and outgoing email messages: directionality is determined by IP addresses of connecting clients and servers, rather than the email addresses of recipients.

- **Incoming connections** consist of those destined for the SMTP servers that are protected domains of the FortiMail unit. For example, if the FortiMail unit is configured to protect the SMTP server whose IP address is 10.1.1.1, the FortiMail unit treats all SMTP connections destined for 10.1.1.1 as incoming. For information about configuring protected domains, see [“config domain-setting” on page 81](#).
- **Outgoing connections** consist of those destined for SMTP servers that the FortiMail unit has not been configured to protect. For example, if the FortiMail unit is ***not*** configured to protect the SMTP server whose IP address is 192.168.1.1, all SMTP connections destined for 192.168.1.1 will be treated as outgoing, regardless of their origin.

Syntax

```
config system interface
  edit <physical_interface_str>, <logical_interface_str>, or
    loopback
      set allowaccess {ping http https snmp ssh telnet}
      set ip <ipv4mask>
      set ip6 <ipv6mask>
      set mac-addr <xx.xx.xx.xx.xx.xx>
      set mode {static | dhcp}
      set mtu <mtu_int>
      set proxy-smtp-in-mode {pass-through | drop | proxy}
      set proxy-smtp-local status {enable | disable}
      set proxy-smtp-out-mode {pass-through | drop | proxy}
      set speed {auto | 10full | 10half | 100full | 100half |
        1000full}
      set status {down | up}
      set type {vlan | redundant}
      set vlanid <int>
      set redundant-link-monitor {mii-link | arp-link}
      set redundant-arp-ip <ip_addr>
      set redundant-member <member_interface_str>
    end
end
```

Variable	Description	Default
<physical_interface_str>	Enter the name of the physical network interface, such as port1.	
<logical_interface_str>	Enter a name for the VLAN or redundant interface. Then set the interface type.	
loopback	<p>A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.</p> <p>The FortiMail's loopback IP address does not depend on one specific external port, and is therefore possible to access it through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiMail unit.</p> <p>The loopback interface is useful when you use a layer 2 load balancer in front of several FortiMail units. In this case, you can set the FortiMail loopback interface's IP address the same as the load balancer's IP address and thus the FortiMail unit can pick up the traffic forwarded to it from the load balancer.</p>	

Variable	Description	Default
allowaccess {ping http https snmp ssh telnet}	<p>Enter one or more of the following protocols to add them to the list of protocols permitted to administratively access the FortiMail unit through this network interface:</p> <ul style="list-style-type: none"> • <code>ping</code>: Allow ICMP ping responses from this network interface. • <code>http</code>: Allow HTTP access to the web-based manager, webmail, and per-recipient quarantines. Caution: HTTP connections are <i>not</i> secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. • <code>https</code>: Allow secure HTTP (HTTPS) access to the web-based manager, webmail, and per-recipient quarantines. • <code>snmp</code>: Allow SNMP v2 access. For more information, see “system snmp community” on page 301, “system snmp sysinfo” on page 303, and “system snmp threshold” on page 303. • <code>ssh</code>: Allow SSH access to the CLI. • <code>telnet</code>: Allow Telnet access to the CLI. Caution: Telnet connections are <i>not</i> secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. <p>To control SMTP access, configure access control rules and session profiles. For details, see “policy access-control receive” on page 152 and “profile session” on page 229.</p>	Varies by the network interface.
ip <ipv4mask>	<p>Enter the IP address and netmask of the network interface.</p> <p>If the FortiMail unit is in transparent mode, <i>IP/Netmask</i> may alternatively display <i>bridging</i>. This means that the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, <i>IP</i> and <i>Netmask</i> may alternatively display <i>bridged (isolated)</i> while the effective operating mode is <i>slave</i> and therefore the network interface is currently disconnected from the network, or <i>bridging (waiting for recovery)</i> while the effective operating mode is <i>failed</i> and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity.</p>	

Variable	Description	Default
ip6 <ipv6mask>	<p>Enter the IPv6 address and netmask of the network interface.</p> <p>If the FortiMail unit is in transparent mode, <i>IP/Netmask</i> may alternatively display <i>bridging</i>. This means that the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, <i>IP</i> and <i>Netmask</i> may alternatively display <i>bridged (isolated)</i> while the effective operating mode is <i>slave</i> and therefore the network interface is currently disconnected from the network, or <i>bridging (waiting for recovery)</i> while the effective operating mode is <i>failed</i> and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity.</p>	
mac-addr <xx.xx.xx.xx.xx.x x>	Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx.	Factory set
mode {static dhcp}	<p>Enter the interface mode.</p> <p>DHCP mode applies only if the FortiMail unit is operating in gateway mode or server mode.</p>	static
mtu <mtu_int>	<p>Enter the maximum packet or Ethernet frame size in bytes.</p> <p>If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance.</p> <p>The valid range is from 576 to 1500 bytes.</p>	1500

Variable	Description	Default
proxy-smtp-in-mode {pass-through drop proxy}	<p>Enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are <i>incoming</i> to the IP addresses of email servers belonging to a protected domain:</p> <ul style="list-style-type: none"> <code>pass-through</code>: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. <code>drop</code>: Drop the connection. <code>proxy</code>: Proxy or relay the connection. Once intercepted, policies determine any further scanning or logging actions. For more information, see “policy ip” on page 160, “policy recipient” on page 163, and “config policy recipient” on page 95 <p>Note: Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered <code>proxy</code> more than once for each interface and/or directionality. For an example, see the FortiMail Administration Guide.</p> <p>This option is only available in transparent mode.</p>	proxy
proxy-smtp-local status {enable disable }	<p>Enable to allow connections destined for the FortiMail unit itself.</p> <p>This option is only available in transparent mode.</p>	disable
proxy-smtp-out-mode {pass-through drop proxy}	<p>Enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are <i>incoming</i> to the IP addresses of email servers belonging to a protected domain:</p> <ul style="list-style-type: none"> <code>pass-through</code>: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. <code>drop</code>: Drop connections. <code>proxy</code>: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see “policy ip” on page 160. <p>Note: Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered <code>proxy</code> more than once for each interface and/or directionality. For an example, see the FortiMail Administration Guide.</p> <p>This option is only available in transparent mode.</p>	pass-through
redundant-arp-ip <ip_addr>	<p>Enter the redundant interface ARP monitoring IP target.</p> <p>This option is only available when you choose the <code>arp-link</code> monitoring parameter. See redundant-link-monitor {mii-link arp-link}.</p>	

Variable	Description	Default
type {vlan redundant}	<p>vlan: A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.</p> <p>Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.</p> <p>One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet.</p> <p>Also configure <code>redundant-link-monitor {mii-link arp-link}</code> and <code>redundant-member <member_interface_str></code>.</p> <p>redundant: On the FortiMail unit, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails.</p> <p>In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.</p> <p>Also configure <code>vlanid <int></code>.</p>	
redundant-link-monitor {mii-link arp-link}	<p>Configure the parameters to monitor the connections of the redundant interfaces. This option is only available when you choose the <code>redundant</code> interface type.</p> <p>mii-link: Media Independent Interface is an abstract layer between the operating system and the NIC which detects whether the failover link is running.</p> <p>arp-link: Address Resolution Protocol periodically checks whether the remote interface is reachable. Also configure <code>redundant-arp-ip <ip_addr></code>.</p>	mii-link
redundant-member <member_interface_str>	<p>Enter the redundant member for the failover configuration.</p> <p>This option is only available when you choose the <code>redundant</code> interface type.</p>	

Variable	Description	Default
vlanid <int>	Enter the Vlan ID for logically separating devices on a network into smaller broadcast domains. This option is only available when you choose the <code>vlan</code> interface type.	
speed {auto 10full 10half 100full 100half 1000full}	Enter the speed of the network interface. Note: Some network interfaces may not support all speeds.	auto
status {down up}	Enter either <code>up</code> to enable the network interface to send and receive traffic, or <code>down</code> to disable the network interface.	up

Related topics

- [sensitive data](#)
- [system admin](#)

system mailserver

Use this command to configure the system-wide mail settings.

Syntax

```
config system mailserver
  config mail-queue
    edit {default | incoming | outgoing}
      set queue-dsn-timeout <timeout_int>
      set queue-retry <interval_int>
      set queue-timeout <timeout_int>
      set queue-warning <first-dsn_int>
    end
  set deadmail-expiry <time_int>
  set default-auth-domain <domain_name>
  set defer-delivery-starttime <time_str>
  set defer-delivery-stoptime <time_str>
  set delivery-esmtp {no | yes}
  set delivery-failure-conditions {dns-failure |
    mta-failure-permanent | mta-failure-temporary |
    network-failure-connection | network-failure-other}
  set delivery-failure-handling-option {normal | relay-to-host}
  set delivery-failure-host <host_name>
  set delivery-failure-min-age <minute_int>
  set dsn-sender-address <email_str>
  set dsn-sender-displayname <name_str>
  set dsn-status {enable | disable}
  set imap-service {enable | disable}
  set ldap-domaincheck {enable | disable}
  set ldap-domaincheck-auto-associate {enable | disable}
  set ldap-domaincheck-internal-domain <domain_str>
  set ldap-domaincheck-profile <profile_str>
  set local-domain-name <local-domain_str>
  set pop3-port <port_int>
  set pop3-service {enable | disable}
  set queue-dsn-timeout <timeout_int>
  set queue-retry <interval_int>
  set queue-timeout <timeout_int>
  set queue-warning <first-dsn_int>
  set relay-server-name <relay_name>
  set relay-server-status {enable | disable}
  set smtp-auth {enable | disable}
  set smtp-auth-over-tls {enable | disable}
  set smtp-auth-smtps {enable | disable}
  set smtp-max-connections <connection_int>
  set smtp-max-hop-count <number>
  set smtp-msa {enable | disable}
  set smtp-msa-port <port_int>
  set smtp-port <port_int>
  set smtp-service {enable | disable}
  set smtps-port <port_int>
  set smtps-tls-status {enable | disable}
```

```

set timeout-connect <seconds_int>
set timeout-greeting <seconds_int>
end

```

Variable	Description	Default
deadmail-expiry <time_int>	Enter the number of days to keep permanently undeliverable email in the dead mail folder. Dead mail has both incorrect recipient and sender email addresses, and can neither be delivered nor the sender notified. The valid range is from 1 to 365 days.	1
default-auth-domain <domain_name>	Enter the domain to use for default authentication.	
{default incoming outgoing}	Select the queue you want to configure.	default
defer-delivery-starttime <time_str>	Enter the time that the FortiMail unit will begin to process deferred oversized email, using the format hh:mm, where hh is the hour according to a 24-hour clock, and mm is the minutes.	00:00
defer-delivery-stop-time <time_str>	Enter the time that the FortiMail unit will stop processing deferred oversized email, using the format hh:mm, where hh is the hour according to a 24-hour clock, and mm is the minutes.	00:00
delivery-esmtp {no yes}	Enter either: <ul style="list-style-type: none"> yes: Disable the FortiMail unit from delivering email using ESMTP, and use standard SMTP instead. no: Enable the FortiMail unit to deliver email using ESMTP if the SMTP server to which it is connecting supports the protocol. 	no
delivery-failure-conditions {dns-failure mta-failure-permanent mta-failure-temporary network-failure-connection network-failure-other}	Specify the type of failed network connections the backup relay should take over and retry.	
delivery-failure-handling-option {normal relay-to-host}	When email delivery fails, you can choose to use the mail queue settings to handle the temporary or permanent failures. You can also try another relay that you know might work. normal: Enter this option if you want to queue the email and use the mail queue settings. relay-to-host: Enter another relay (backup relay) that you want to use for failed deliveries.	normal
delivery-failure-host <host_name>	Enter a host to relay email when access to original mail host fails.	

Variable	Description	Default
delivery-failure-min-age <minute_int>	Enter the time in minutes the undelivered email should wait in the normal queue before trying the backup relay.	30
dsn-sender-address s <email_str>	Enter the sender email address in delivery status notification (DSN) email messages sent by the FortiMail unit to notify email users of delivery failure. If this string is empty, the FortiMail unit sends DSN from the default sender email address of "postmaster@example.com", where "example.com" is the domain name of the FortiMail unit.	
dsn-sender-displayname yname <name_str>	Enter the display name of the sender email address for DSN. If this string is empty, the FortiMail unit uses the display name "postmaster".	
dsn-status {enable disable }	Enable to allow DSN email generation.	disable
imap-service {enable disable }	Enable to allow IMAP service.	disable
ldap-domaincheck {enable disable }	Enable to verify the existence of domains that have not been configured as protected domains. Also configure <code>ldap-domaincheck-profile <profile_str></code> and <code>ldap-domaincheck-auto-associate {enable disable}</code> . To verify the existence of unknown domains, the FortiMail unit queries an LDAP server for a user object that contains the email address. If the user object exists, the verification is successful, the action varies by configuration of <code>ldap-domaincheck-auto-associate {enable disable}</code> .	disable
ldap-domaincheck-auto-associate {enable disable }	If <code>ldap-domaincheck</code> is enable, select whether to enable or disable automatic creation of domain associations. <ul style="list-style-type: none">• <code>enable</code>: The FortiMail unit automatically adds the unknown domain as a domain associated of the protected domain selected in <code>ldap-domaincheck-internal-domain <domain_str></code>.• <code>disable</code>: If the DNS lookup of the unknown domain name is successful, the FortiMail unit routes the email to the IP address resolved for the domain name during the DNS lookup. Because the domain is not formally defined as a protected domain, the email is considered to be outgoing, and outgoing recipient-based policies are used to scan the email. For more information, see "policy recipient" on page 163.	disable

Variable	Description	Default
ldap-domaincheck-internal-domain <domain_str>	If ldap-domaincheck is enable, and ldap-domaincheck-auto-associate is enable, enter name of the protected domain with which successfully verified domains will become associated.	
ldap-domaincheck-profile <profile_str>	If ldap-domaincheck is enable, enter the name of the LDAP profile to use when verifying unknown domains.	
local-domain-name <local-domain_str>	Enter the name of the domain to which the FortiMail unit belongs, such as example.com. This option applies only if the FortiMail unit is operating in server mode.	
pop3-port <port_int>	Enter the port number on which the FortiMail unit's POP3 server will listen for POP3 connections. The default port number is 110. This option applies only if the FortiMail unit is operating in server mode.	110
pop3-service {enable disable }	Enable to allow POP3 service.	disable
queue-dsn-timeout <timeout_int>	Enter the maximum number of days a delivery status notification (DSN) message can remain in the mail queues. If the maximum time is set to zero (0) days, the FortiMail unit attempts to deliver the DSN only once. After the maximum time has been reached, the DSN email is moved to the dead mail folder. The valid range is from zero to ten days.	5
queue-retry <interval_int>	Enter the number of minutes between delivery retries for email messages in the deferred and spam mail queues. The valid range is from 10 to 120 minutes.	27
queue-timeout <timeout_int>	Enter the maximum number of hours that deferred email messages can remain in the deferred or spam mail queue, during which the FortiMail unit periodically retries to send the message. After the maximum time has been reached, the FortiMail unit will send a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable. The valid range is from 1 to 240 hours.	120
queue-warning <first-dsn_int>	Enter the number of hours after an initial failure to deliver an email message before the FortiMail unit sends the first delivery status notification (DSN) email message to notify the sender that the email message has been deferred. After sending this initial DSN, the FortiMail unit will continue to retry sending the email until reaching the limit configured in timeout. The valid range is from 1 to 24 hours.	4

Variable	Description	Default
relay-server-name <relay_name>	Specify the relay server to deliver outgoing email.	
relay-server-status {enable disable}	If enabled, the relay server will be used to deliver outgoing email. If disabled, the FortiMail built-in MTA will be used.	disable
smtp-auth {enable disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTP.	enable
smtp-auth-over-tls {enable disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTP over TLS.	enable
smtp-auth-smtps {enable disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTPS (SMTP with SSL).	enable
smtp-max-connections <connection_int>	Enter the maximum number of concurrent SMTP connections that FortiMail can accept from the SMTP clients.	Platform dependent
smtp-max-hop-count <number>	Enter the maximum number of hops that FortiMail can accept from the SMTP connections. Valid range is 1 to 200.	30
smtp-msa {enable disable}	Enable to allow your email clients to use SMTP for message submission on a separate TCP port number from deliveries or mail relay by MTAs. For details on message submission by email clients as distinct from SMTP used by MTAs, see RFC 2476 .	disable
smtp-msa-port <port_int>	Enter the TCP port number on which the FortiMail unit listens for email clients to submit email for delivery.	587
smtp-port <port_int>	Enter the port number on which the FortiMail unit's SMTP server will listen for SMTP connections.	25
smtp-service {enable disable}	Enable to allow SMTP service.	disable
smtps-port <port_int>	Enter the port number on which the FortiMail unit's built-in MTA listens for secure SMTP connections.	465
smtps-tls-status {enable disable}	Enable to allow SSL- and TLS-secured connections from SMTP clients that request SSL/TLS. When disabled, SMTP connections with the FortiMail unit's built-in MTA must occur as clear text, unencrypted.	disable

Variable	Description	Default
timeout-connect <seconds_int>	<p>Enter the maximum amount of time to wait, after the FortiMail unit initiates it, for the receiving SMTP server to establish the network connection.</p> <p>The valid range is 10 to 120.</p> <p>Note: This timeout applies to all SMTP connections, regardless of whether it is the first connection to that SMTP server or not.</p>	30
timeout-greeting <seconds_int>	<p>Enter the maximum amount of time to wait for an SMTP server to send SMTP reply code 220 to the FortiMail unit.</p> <p>The valid range is 10 to 360.</p> <p>Note: RFC 2821 recommends a timeout value of 5 minutes (300 seconds). For performance reasons, you may prefer to have a smaller timeout value, which reduces the amount of time spent waiting for sluggish SMTP servers. However, if this causes your FortiMail unit to be unable to successfully initiate an SMTP session with some SMTP servers, consider increasing the timeout.</p>	30

Related topics

- [system route](#)

system password-policy

Use this command to configure password policy for administrators, FortiMail Webmail users, and IBE encrypted email users.

Syntax

```
config system password-policy
    set status {enable | disable}
    set apply-to {admin-user | ibe-user | local-mail-user}
    set minimum-length <minimum_int>
    set must-contain
        {upper-case-letter | lower-case-letter | number | non-alphanumeric}
end
```

Variable	Description	Default
status {enable disable }	Select to enable the password policy.	
apply-to {admin-user ibe -user local-mail-user}	Select where to apply the password policy: admin_user — Apply to administrator passwords. If any password does not conform to the policy, require that administrator to change the password at the next login. local-mail-user — Apply to FortiMail webmail users' passwords. If any password does not conform to the policy, require that user to change the password at the next login. ibe-user — Apply to the passwords of the users who access the FortiMail unit to view IBE encrypted email. If any password does not conform to the policy, require that user to change the password at the next login.	
minimum-length <minimum_int>	Set the minimum acceptable length for passwords.	8
must-contain {upper-case-letter lower-case-letter number non-alphanumeric}	Select any of the following special character types to require in a password. Each selected type must occur at least once in the password. <ul style="list-style-type: none">• upper-case-letter — A, B, C, ... Z• lower-case-letter — a, b, c, ... z• number — 0, 1, 2, 3, 4, 5, 6, 7 8, 9• non-alphanumeric — punctuation marks, @, #, ... %	

Related topics

- [system mailserver](#)

system port-forwarding

FortiMail port forwarding allows remote computers, for example, computers on the Internet, to connect to a specific computer or service within a private local area network (LAN). Port Forwarding is useful when FortiMail is deployed as a gateway and you want external users to access an internal server via FortiMail.

For example, FortiMail port1 is connected to the Internet and its IP address 192.168.37.4, port 7000, is mapped to 10.10.10.42, port 8000, on a private network. Attempts to communicate with 192.168.37.4, port 7000, from the Internet are translated and sent to 10.10.10.42, port 8000, by the FortiMail unit. The computers on the Internet are unaware of this translation and see a single computer at 192.168.37.4, port 7000, rather than the 10.10.10.42 network behind the FortiMail unit.

Before you do the mapping, make sure both ports are open.

Syntax

```
config system port-forwarding
  edit <route_int>
    set destination <destination_ipv4mask>
    set gateway <gateway_ipv4>
  end
```

Variable	Description	Default
<number>	Enter the index number of the entry.	
dst-host <calss_ip>	Enter the IP address of the host where the packets will be forwarded.	0.0.0.0
dst-port <port_number>	Enter the port number of the destination host.	0
host <class_ip>	Enter the IP address of the FortiMail interface where the packets are received.	0.0.0.0
port <port_number>	Enter the port number on the FortiMail interface where the packets are received.	0
protocol {tcp udp both}	Specify the protocol of the traffic.	tcp

system route

Use this command to configure static routes.

Syntax

```
config system route
  edit <route_int>
    set destination <destination_ipv4mask>
    set gateway <gateway_ipv4>
    set interface <interface_name>
  end
```

Variable	Description	Default
<route_int>	Enter the index number of the route in the routing table.	
destination <destination_ipv4 mask>	Enter the destination IP address and netmask of traffic that will be subject to this route, separated with a space. To indicate all traffic regardless of IP address and netmask, enter 0.0.0.0 0.0.0.0.	0.0.0.0 0.0.0.0
gateway <gateway_ipv4>	Enter the IP address of the gateway router.	0.0.0.0
interface <interface_name>	Enter the interface name that you want to add the static route to.	

Related topics

- [system mailserver](#)

system saml

Use this command to enable and configure SAML SSO.

Syntax

```
config system saml
  set status {enable | disable}
  set idp-metadata-url <url>
end
```

Variable	Description	Default
status {enable disable}	Enable or disable the feature.	disable
idp-metadata-url <url>	Specify the URL to retrieve the IDP metadata.	

system scheduled-backup

Use this command to configure system backup.

Syntax

```
config system scheduled-backup
  set destination...
end
```

Variable	Description	Default
destination...	Configure the destination server and schedule.	

system security authserver

Use this command to modify the tracking functions used to prevent password guessing attempts. The sender IP addresses in the exempt list will bypass the security checking.

Syntax

```
config system security authserver
  config exempt-list
    edit auth_exempt_id
      set sender-ip-mask
    end
  set status {disable | enable | monitor-only}
end
```

Variable	Description	Default
auth_exempt_id	Enter the ID for the list.	
sender-ip-mask	Enter the sender's IP address.	
status	Enable or disable this list.	

system snmp community

Use this command to configure simple network management protocol (SNMP) v1/2 settings.

These commands apply only if the SNMP agent is enabled. For details, see [status {enable | disable}](#).

Syntax

```
config system snmp community
  edit <index_int>
    config host
      edit <index_int>
        set ip <address_ipv4>
        set name <name_str>
        set queryportv1 <port_int>
        set queryportv2c <port_int>
        set queryv1-status {enable | disable}
        set queryv2c-status {enable | disable}
        set status {enable | disable}
        set trapevent {cpu | deferred-queue | ha | ip-change | logdisk |
          maildisk | mem | raid | remote-storage | spam | system |
          virus}
        set trapportv1_local <port_int>
        set trapportv1_remote <port_int>
        set trapportv2c_local <port_int>
        set trapportv2c_remote <port_int>
        set trapv1_status {enable | disable}
        set trapv2c_status {enable | disable}
      end
    end
  end
```

Variable	Description	Default
<index_int>	Enter the index number of the SNMP community.	
<index_int>	Enter the index number of the SNMP monitor.	
ip <address_ipv4>	Enter the IP address of the SNMP monitor. The FortiMail unit will, if traps are enabled, send traps to this IP address, and, if queries are enabled, receive queries from this IP address.	
name <name_str>	Enter the name of the SNMP community	
queryportv1 <port_int>	Enter the TCP port on which to listen for SNMPv1 queries from the SNMP monitor.	161
queryportv2c <port_int>	Enter the TCP port on which to listen for SNMPv2c queries from the SNMP monitor.	161
queryv1-status {enable disable }	Enable to allow the FortiMail unit to receive SNMPv1 queries from the SNMP monitor.	enable
queryv2c-status {enable disable }	Enable to allow the FortiMail unit to receive SNMPv2c queries from the SNMP monitor.	enable

Variable	Description	Default
status {enable disable }	Enable to activate the SNMP community.	disable
trapevent {cpu deferred-queue ha ip-change logdisk maildisk mem raid remote-storage spam system virus}	<p>Enter one or more of the following events that will generate a trap when the event occurs or when its threshold is reached:</p> <ul style="list-style-type: none"> • cpu: CPU usage threshold • deferred-queue: Deferred queue threshold • ha: High availability (HA) event • ip-change: Interface IP address change • logdisk: Log disk space low threshold • maildisk: Mail disk space low threshold • mem: Memory low threshold • raid: RAID event • remote-storage: NAS storage related events • spam: Spam threshold • system: System events, such as a change in the state of hardware, power failure and so on. • virus: Virus threshold <p>Note: Since FortiMail checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiMail checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.</p> <p>To set SNMP trap thresholds for the event types that use them, see “system snmp threshold” on page 303.</p>	cpu deferred-queue ha logdisk maildisk mem raid remote-storage system
trapportv1_local <port_int>	Enter the TCP port that the FortiMail unit will use to send SNMP v1 traps to SNMP monitors.	162
trapportv1_remote <port_int>	Enter the TCP port that the FortiMail unit will use to send SNMP v1 traps to SNMP monitors.	162
trapportv2c_local <port_int>	Enter the TCP port that the FortiMail unit will use to send SNMP v2c traps to SNMP monitors.	162
trapportv2c_remote <port_int>	Enter the TCP port that the FortiMail unit will use to send SNMP v2c traps to SNMP monitors.	162
trapv1_status {enable disable }	Enable to activate sending SNMP v1 traps to the SNMP monitor.	enable
trapv2c_status {enable disable }	Enable to activate sending SNMP v2c traps to the SNMP monitor.	enable

Related topics

- [system snmp sysinfo](#)
- [system snmp threshold](#)

system snmp sysinfo

Use this command to enable or disable the SNMP agent on the FortiMail unit, and to configure the location, description, engine ID, and contact information.

Syntax

```
config system snmp sysinfo
  set contact <contact_str>
  set description <description_str>
  set engine-id <id_str>
  set location <location_str>
  set status {enable | disable}
end
```

Variable	Description	Default
contact <contact_str>	Enter the contact information for the administrator of this FortiMail unit, such as 'admin@example.com'.	
description <description_str>	Enter a description for the FortiMail unit that will uniquely identify it to the SNMP monitor, such as 'FortiMail-400 Rack 1'.	
engine-id <id_str>	Enter the SNMP engine ID on the FortiMail unit.	
location <location_str>	Enter the location of this FortiMail unit, such as 'NOC_Floor2'.	
status {enable disable }	Enable to activate the SNMP agent.	enable

Related topics

- [system snmp community](#)
- [system snmp threshold](#)

system snmp threshold

Use this command to configure the event types that trigger an SNMP trap.

Syntax

```
config system snmp threshold
  set {cpu | deferred-queue | logdisk | maildisk | mem | spam |
      virus} <trigger_int> <threshold_int> <sample_period_int>
      <sample_frequency_int>
end
```

Variable	Description	Default
<pre>{cpu deferred-queue logdisk maildisk mem spam virus} <trigger_int> <threshold_int> <sample_period_int> <sample_frequency_int></pre>	<p>Specify the trap event, such as cpu or spam, then specify the following threshold values:</p> <ul style="list-style-type: none"> trigger_int: You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger. threshold_int: Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period. sample_period_int: Sets the time period in seconds during which the FortiMail unit SNMP agent counts the number of triggers that occurred. This value should not be less than the Sample Frequency value. sample_frequency_int: Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the Sample Period value. 	<pre>cpu: 80 3 600 30 mem: 80 3 600 30 logdisk: 90 1 7200 3600 maildisk : 90 1 7200 3600 virus: 10 600 spam: 60 600</pre>

Related topics

- [system snmp community](#)
- [system snmp sysinfo](#)

system snmp user

Use this command to configure SNMP v3 user settings.

SNMP v3 adds more security by using authentication and privacy encryption. You can specify an SNMP v3 user on FortiMail so that SNMP managers can connect to the FortiMail unit to view system information and receive SNMP traps.

Syntax

```

config system snmp user
  edit <user_name>
    set query-status {enable | disable}
    set query-port <port_number>
    set security-level {authnopriv | authpriv | noauthnopriv}
    set auth-proto {sha1 | md5}
    set aut-pwd <password>
    set status {enable | disable}
    set trap-status {enable | disable}
    set trapevent {cpu | deferred-queue | ha | ip-change | logdisk |
      mem | raid | remote-storage | spam | system | virus}
    set trapport-local <port_number>
    set trapport-remote <port_number>
  config host
    edit <host_no>
      set ip <class_ip>
    end
  end
end

```

Variable	Description	Default
<user_name>	Enter a name to identify the SNMP user on FortiMail.	
query-status {enable disable}	Enable to allow SNMP v3 query from the SNMP managers. Also configure the query port as described below.	disable
query-port <port_number>	Specify the port number used to listen to queries from the SNMP manager.	161
security-level {authnopriv authpriv noauthnopriv}	<p>Choose one of the three security levels for the communication between FortiMail and the SNMP manager.</p> <ul style="list-style-type: none"> noauthnotpriv (no authentication, no privacy): This option is similar to SNMP v1 and v2. authnopriv (authentication, no privacy): This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiMail. You must also specify the authentication protocol (either SHA1 or MD5). authpriv (authentication, privacy): This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiMail must match. 	
auth-proto {sha1 md5}	Specify the authentication protocol if you choose authentication for the security level. Otherwise, this option is not displayed.	
aut-pwd <password>	Specify the authentication password if you choose authentication for the security level. Otherwise, this option is not displayed.	

Variable	Description	Default
status {enable disable}	Enable or disable the SNMP v3 user on FortiMail.	disable
trap-status {enable disable}	Enable to activate traps on FortiMail.	disable
trapevent {cpu deferred-queue ha ip-change logdisk mem raid remote-storage spam system virus}	<p>Enter one or more of the following events that will generate a trap when the event occurs or when its threshold is reached:</p> <ul style="list-style-type: none"> cpu: CPU usage threshold deferred-queue: Deferred queue threshold ha: High availability (HA) event ip-change: Interface IP address change logdisk: Log disk space low threshold maildisk: Mail disk space low threshold mem: Memory low threshold raid: RAID event remote-storage: NAS storage related events spam: Spam threshold system: System events, such as a change in the state of hardware, power failure and so on. virus: Virus threshold <p>Note: Since FortiMail checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiMail checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent.</p> <p>To set SNMP trap thresholds for the event types that use them, see “system snmp threshold” on page 303.</p>	cpu deferred-queue ha logdisk maildisk mem raid remote-storage system
trapport-local <port_number>	Enter the local port number for sending traps.	162
trapport-remote <port_number>	Enter the remote port number that listens to SNMP traps on the SNMP manager.	162
<host_no>	Enter an index number for the SNMP manager.	
ip <class_ip>	Enter the IP address of the SNMP manager.	

Related topics

- [system snmp community](#)
- [system snmp sysinfo](#)

system time manual

Use this command to manually configure the system time of the FortiMail unit.

Accurate system time is required by many features of the FortiMail unit, including but not limited to log messages and SSL-secured connections.

This command applies only if NTP is disabled. Alternatively, you can configure the FortiMail unit to synchronize its system time with an NTP server. For details, see [“system time ntp” on page 307](#).

Syntax

```
config system time manual
    set daylight-saving-time {disable | enable}
    set zone <zone_int>
end
```

Variable	Description	Default
daylight-saving-time {disable enable}	Enable to automatically adjust the system time for daylight savings time (DST).	enable
zone <zone_int>	Enter the number that indicates the time zone in which the FortiMail unit is located.	12

Related topics

- [system time ntp](#)

system time ntp

Use this command to configure the FortiMail unit to synchronize its system time with a network time protocol (NTP) server.

Accurate system time is required by many features of the FortiMail unit, including but not limited to log messages and SSL-secured connections.

Alternatively, you can manually configure the system time of the FortiMail unit. For details, see [“system time manual” on page 306](#).

Syntax

```
config system time ntp
    set ntpserver {<address_ipv4> | <fqdn_str>}
    set ntpsync {enable | disable}
    set syncinterval <interval_int>
end
```

Variable	Description	Default
ntpserver {<address_ipv4> <fqdn_str>}	Enter either the IP address or fully qualified domain name (FQDN) of an NTP server. You can add a maximum of 10 NTP servers. The FortiMail unit uses the first NTP server based on the selection mechanism of the NTP protocol. To locate a public NTP server, visit http://www.ntp.org/ .	pool.ntp.org
ntpsync {enable disable}	Enable to synchronize the FortiMail unit with an NTP server, instead of manually configuring the system time.	enable
syncinterval <interval_int>	Enter the interval in minutes between synchronizations of the system time with the NTP server. The valid range is from 1 to 1440 minutes.	60

Related topics

- [system time manual](#)

system webmail-language

Use this command to create or rename a webmail language.

When you create a webmail language, it is initialized using by copying the English language file. For example, the location in webmail whose resource ID is `mail_box` contains the value `Mail Box`. To finish creation of your webmail language, you must replace the English values with your translation or customized term by either:

- editing the resource values for each resource ID in the web-based manager
- downloading, editing, then uploading the language resource file

For information on how to edit a webmail language, see the [FortiMail Administration Guide](#).

Syntax

```
config system webmail-language
    edit en_name <language-name-en_str>
        set name <language-name_str>
    end
```

Variable	Description	Default
en_name <language-name-en_str>	Enter the name of the language in English, such as 'French'. Available languages vary by whether or not you have installed additional language resource files.	No default.
name <language-name_str>	Enter the name of the language, such as 'Français'.	No default.

Related topics

- [config user mail](#)

system wccp settings

FortiMail and FortiGate support Web Cache Communication Protocol (WCCP) to redirect SMTP traffic from FortiGate to FortiMail. If the FortiGate unit is configured to redirect SMTP traffic to FortiMail for antispam scanning (for details, see the FortiGate documentation), on the FortiMail side, you must do corresponding configurations to accept the SMTP traffic from FortiGate.

Syntax

```
config system wccp settings
    set authentication
    set id
    set local-ip
    set password
    set remote-ip
    set status
end
```

Variable	Description	Default
authentication	Enable or disable authentication.	No default.
id	Enter the ID of the tunnel.	No default.
local-ip	Enter the ip address of the local interface.	No default
password	Enter the authentication password.	No default
remote-ip	Enter the ip address of the remote server.	No default
status	Enable or disable WCCP mode.	

user alias

Use this command to configure email address aliases.

Aliases are sometimes also called distribution lists, and may translate one email address to the email addresses of several recipients, also called members, or may be simply a literal alias — that is, an alternative email address that resolves to the real email address of a single email user.

For example, groupa@example.com might be an alias that the FortiMail unit will expand to user1@example.com and user2@example.com, having the effect of distributing an email message to all email addresses that are members of that alias, while john.smith@example.com might be an alias that the FortiMail unit translates to j.smith@example.com. In both cases, the FortiMail unit converts the alias in the recipient fields of incoming email messages into the member email addresses of the alias, each of which are the email address of an email user that is locally deliverable on the SMTP server or FortiMail unit.

Alternatively, you can configure an LDAP profile in which the alias query is enabled. For details, see “[profile ldap](#)” on page 211.

Syntax

```
config user alias
    edit name <email-alias_str>
        set member <recipient_str>
    end
```

Variable	Description	Default
name <email-alias_str>	Enter the email address that is the alias, such as alias1@example.com.	No default.
member <recipient_str>	Enter a recipient email addresses to which the alias will translate or expand.	No default.

Related topics

- [user map](#)
- [user pki](#)

user map

Use this command to configure email address mappings.

Address mappings are bidirectional, one-to-one or many-to-many mappings. They can be useful when:

- you want to hide a protected domain's true email addresses from recipients
- a mail domain's domain name is not globally DNS-resolvable, and you want to replace the domain name with one that is
- you want to rewrite email addresses

Like aliases, address mappings translate email addresses. They do not translate many email addresses into a single email address. However, **unlike** aliases:

- Mappings cannot translate one email address into many.
- Mappings cannot translate an email address into one that belongs to an unprotected domain. (This restriction applies to locally defined address mappings only. This is not enforced for mappings defined on an LDAP server.)
- Mappings are applied bidirectionally, when an email is outgoing as well as when it is incoming to the protected domain.
- Mappings may affect both sender and recipient email addresses, and may affect those email addresses in both the message envelope and the message header, depending on the match condition.

The following table illustrates the sequence in which parts of each email are compared with address mappings for a match, and which locations' email addresses are translated if a match is found.



Both RCPT TO: and MAIL FROM: email addresses are always evaluated for a match with an address mapping. If both RCPT TO: and MAIL FROM: contain email addresses that match the mapping, both mapping translations will be performed.

Table 9: Match evaluation and rewrite behavior for email address mappings

Order of evaluation	Match condition	If yes...	Rewrite to...
1	Does <code>RCPT TO:</code> match an external email address?	Replace <code>RCPT TO:</code> .	Internal email address
2	Does <code>MAIL FROM:</code> match an internal email address?	For each of the following, if it matches an internal email address, replace it: <ul style="list-style-type: none"> • <code>MAIL FROM:</code> • <code>RCPT TO:</code> • <code>From:</code> • <code>To:</code> • <code>Return-Path:</code> • <code>Cc:</code> • <code>Reply-To:</code> • <code>Return-Receipt-To:</code> • <code>Resent-From:</code> • <code>Resent-Sender:</code> • <code>Delivery-Receipt-To:</code> • <code>Disposition-Notification-To:</code> 	External email address

For example, you could create an address mapping between the internal email address `user1@marketing.example.net` and the external email address `sales@example.com`. The following effects would be observable on the simplest case of an outgoing email and an incoming reply:

- **For email from `user1@marketing.example.net` to others:** `user1@marketing.example.net` in both the message envelope (`MAIL FROM:`) and many message headers (`From:`, etc.) would then be replaced with `sales@example.com`. Recipients would only be aware of the email address `sales@example.com`.
- **For email to `sales@example.com` from others:** The recipient address in the message envelope (`RCPT TO:`), but **not** the message header (`To:`), would be replaced with `user1@marketing.example.net`. `user1@marketing.example.net` would be aware that the sender had originally sent the email to the mapped address, `sales@example.com`.

Alternatively, you can configure an LDAP profile to query for email address mappings. For details, see [“profile ldap” on page 211](#).

Syntax

```
config user map
    edit internal-name <pattern_str>
        set external-name <pattern_str>
    end
```

Variable	Description	Default
internal-name <pattern_str>	<p>Enter either an email address, such as <code>user1@example.com</code>, or an email address pattern, such as <code>*@example.com</code>, that exists in a protected domain.</p> <p>This email address will be rewritten into <code>external-name <pattern_str></code> according to the match conditions and effects described in Table 9 on page 311.</p> <p>Note: If you enter a pattern with a wild card (* or ?):</p> <ul style="list-style-type: none"> You must enter a pattern using the same wild card in <code>external-name <pattern_str></code>. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the external address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, * mapped to ? or vice versa), this substitution will fail. <code>external-name <pattern_str></code> must not be within the same protected domain. This could cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable. 	No default.
external-name <pattern_str>	<p>Enter either an email address, such as <code>user2@example.com</code>, or an email address pattern, such as <code>*@example.net</code>, that exists in a protected domain.</p> <p>This email address will be rewritten into <code>internal-name <pattern_str></code> according to the match conditions and effects described in Table 9 on page 311.</p> <p>Note: If you enter a pattern with a wild card (* or ?):</p> <ul style="list-style-type: none"> You must enter a pattern using the same wild card in <code>internal-name <pattern_str></code>. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the internal address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, * mapped to ? or vice versa), this substitution will fail. <code>internal-name <pattern_str></code> must not be within the same protected domain. This could cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable. 	No default.

Related topics

- [system wccp settings](#)

user pki

Use this command to configure public key infrastructure (PKI) users.

A PKI user can be either an email user or a FortiMail administrator. PKI users can authenticate by presenting a valid client certificate, rather than by entering a user name and password.

When the PKI user connects to the FortiMail unit with his or her web browser, the web browser presents the PKI user's certificate to the FortiMail unit. If the certificate is valid, the FortiMail unit then authenticates the PKI user. To be valid, a client certificate must:

- Not be expired
- Not be revoked by either certificate revocation list (CRL) or, if enabled, online certificate status protocol (OCSP)
- Be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail unit
- Contain a "ca" field whose value matches the CA certificate
- Contain a "issuer" field whose value matches the "subject" field in the CA certificate
- Contain a "subject" field whose value contains the subject, or is empty
- If `ldap-query` is `enable`, contain a common name (CN) or Subject Alternative field whose value matches the email address of a user object retrieved using the user query of the LDAP profile

If the client certificate is **not** valid, depending on whether you have configured the FortiMail unit to require valid certificates "[system global](#)" on page 273, authentication will either fail absolutely, or fail over to a user name and password mode of authentication.

If the certificate is valid and authentication succeeds, the PKI user's web browser is redirected to either the web-based manager (for PKI users that are FortiMail administrators) or the mailbox folder that contains quarantined spam (for PKI users that are email users).

After using this command to configure a PKI user, you must also configure the following aspects of the FortiMail unit and the PKI user's computer:

- Import each PKI user's client certificate into the web browser of each computer from which the PKI user will access the FortiMail unit. For details on installing certificates, see the documentation for your web browser.



Control access to each PKI user's computer. Certificate-based PKI authentication controls access to the FortiMail unit based upon PKI certificates, which are installed on each email user or administrator's computer. If anyone can access the computers where those PKI certificates are installed, they can gain access to the FortiMail unit, which can compromise the security of your FortiMail unit.

- Import the CA certificate into the FortiMail unit. For information on uploading a CA certificate, see the [FortiMail Administration Guide](#).
- For PKI users that are FortiMail administrators, select the PKI authentication type and select a PKI user to which the administrator account corresponds. For more information, see "[system admin](#)" on page 249.
- For PKI users that are email users, enable PKI user authentication for the recipient-based policies which match those email users.

This command takes effect only if PKI authentication is enabled by `pki-mode {enable | disable}` in the command "[system global](#)" on page 273.

Syntax

```
config user pki
  edit name <name_str>
    set ca <certificate_str>
    set domain <protected-domain_str>
    set ldap-field {cn | subjectalternative}
    set ldap-profile <profile_str>
    set ldap-query {enable | disable}
    set ocsp-ca <remote-certificate_str>
    set ocsp-check {enable | disable}
    set ocsp-unavailable-action {revoke | ignore}
    set ocsp-url <url_str>
    set subject <subject_str>
  end
```

Variable	Description	Default
name <name_str>	Enter the name of the PKI user.	
ca <certificate_str>	Enter the name of the CA certificate used when verifying the CA's signature of the client certificate. For information on uploading a CA certificate, see the FortiMail Administration Guide .	
domain <protected-domain_str>	Enter the name of the protected domain to which the PKI user is assigned, or enter <code>system</code> if the PKI user is a FortiMail administrator and belongs to all domains configured on the FortiMail unit. For more information on protected domains, see “ dlp scan-rules ” on page 78.	
ldap-field {cn subjectalternative}	Enter the name of the field in the client certificate (either CN or Subject Alternative) which contains the email address of the PKI user, either <code>subjectalternative</code> (if the field is a Subject Alternative) or <code>cn</code> (if the field is a common name). This email address will be compared with the value of the email address attribute for each user object queried from the LDAP directory to determine if the PKI user exists in the LDAP directory. This variable is used only if <code>ldap-query</code> is <code>enable</code> .	subject
ldap-profile <profile_str>	Enter the LDAP profile to use when querying the LDAP server for the PKI user's existence. For more information on LDAP profiles, see “ profile ldap ” on page 211. This variable is used only if <code>ldap-query</code> is <code>enable</code> .	
ldap-query {enable disable}	Enable to query an LDAP directory, such as Microsoft Active Directory, to determine the existence of the PKI user who is attempting to authenticate. Also configure <code>ldap-profile <profile_str></code> and <code>ldap-field {cn subjectalternative}</code> .	disable

Variable	Description	Default
ocsp-ca <remote-certificate_str>	Enter the name of the remote certificate that is used to verify the identity of the OCSP server. For information on uploading a remote (OCSP) certificate, see the <i>FortiMail Administration Guide</i> . This option applies only if <code>ocspverify</code> is enable.	
ocsp-check {enable disable}	Enable to use an Online Certificate Status Protocol (OCSP) server to query whether the client certificate has been revoked. Also configure <code>ocsp-url</code> <url_str>, [<code>ocsp-ca</code> <remote-certificate_str>], and <code>ocsp-unavailable-action</code> {revoke ignore}.	disable
ocsp-unavailable-action {revoke ignore}	Enter the action to take if the OCSP server is unavailable. If set to ignore, the FortiMail unit allows the user to authenticate. If set to revoke, the FortiMail unit behaves as if the certificate is currently revoked, and authentication fails. This option applies only if <code>ocsp-check</code> is enable.	ignore
ocsp-url <url_str>	Enter the URL of the OCSP server. This option applies only if <code>ocsp-check</code> is enable.	
subject <subject_str>	Enter the value which must match the "subject" field of the client certificate. If empty, matching values are not considered when validating the client certificate presented by the PKI user's web browser.	

Related topics

- [system wccp settings](#)
- [user map](#)

execute

`execute` commands perform immediate operations on the FortiMail unit.

This chapter describes the following `execute` commands:

<code>backup</code>	<code>maintain</code>
<code>backup-restore</code>	<code>nslookup</code>
<code>certificate</code>	<code>partitionlogdisk</code>
<code>checklogdisk</code>	<code>ping</code>
<code>checkmaildisk</code>	<code>ping-option</code>
<code>cleanqueue</code>	<code>ping6</code>
<code>create</code>	<code>ping6-option</code>
<code>date</code>	<code>raid</code>
<code>db</code>	<code>reboot</code>
<code>dlp</code>	<code>reload</code>
<code>endpoint</code>	<code>restore as</code>
<code>erase filesystem</code>	<code>restore av</code>
<code>factoryreset disk</code>	<code>restore config</code>
<code>fips</code>	<code>restore image</code>
<code>formatlogdisk</code>	<code>restore mail-queues</code>
<code>formatmaildisk</code>	<code>sched-backup</code>
<code>formatmaildisk_backup</code>	<code>shutdown</code>
<code>forticloud</code>	<code>smtptest</code>
<code>ha commands</code>	<code>ssh</code>
<code>ibe data</code>	<code>storage</code>
<code>ibe user</code>	<code>telnettest</code>
<code>license</code>	<code>traceroute</code>
<code>lvm</code>	<code>update</code>
	<code>user-config</code>
	<code>vm</code>

backup

Use this command to back up the configuration file to either a TFTP server or FortiManager (management-station).



This command does **not** produce a complete backup. For information on how to back up other configuration files such as Bayesian databases, see the [FortiMail Administration Guide](#).

Syntax

```
execute backup {config | full-config | ibe-data | mail-queue |  
               user-config}  
               {tftp <filename_str> <tftp_ipv4> [<password_str>] |  
                management-station [<comments_str>]}
```

Variable	Description	Default
{config full-config ibe-data mail-queue user-config}	Type either: <ul style="list-style-type: none">• config: Back up configuration changes only. The default settings will not be backed up.• full-config: Back up the entire configuration file (no default settings either), including the IBE data and user config.• ibe-data: Back up the IBE data.• mail-queue: Back up the mail queues.• user-config: Back up the user-specific configurations, such as user preferences, personal black/white lists, and secondary addresses. Before backing up, you should update the user configuration file. To update the configurations, see “user-config” on page 352.	No default.
<filename_str>	Type the file name that will be used for the backup file, such as FortiMail_backup.txt.	No default.
<tftp_ipv4>	Type the IP address of the TFTP server.	No default.
[<password_str>]	Type a password that will be used to encrypt the backup file, and which must be provided when restoring the backup file. If you do not provide a password, the backup file is stored as clear text.	No default.
[<comments_str>]	If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (“) or any other punctuation marks.	No default.

Example

This example uploads a password-encrypted partial configuration backup to a TFTP server.

```

FortiMail-400 # execute backup full-config tftp fortimail_backup.cfg
172.16.1. 1 P@ssword1

No user configuration available!

Do you want to continue? (y/n)y

No IBE data available!

Do you want to continue? (y/n)y

System time: Tue Sep 27 13:07:43 2011

Backup with current user defined configuration and ibe data. Do you
want to continue? (y/n)y

Connect to tftp server 172.16.1.1 ...

Please wait...

```

Related topics

- [restore config](#)
- [user-config](#)

backup-restore

Use this command to back up or restore email users' mailboxes. Before using this command, you must specify the backup destination or the restore location first. For details, see [“system backup-restore-mail”](#) on page 253.

Syntax

```

execute backup-restore all-restore
execute backup-restore check-device
execute backup-restore format-device
execute backup-restore old-restore <full_int> <increments_int>
    domain <domain_str> user <user_str>
execute backup-restore restore {domain <domain> user <user> | host
    <host>}
execute backup-restore start
execute backup-restore stop

```

Variable	Description	Default
all-restore	Use this command to restore mail data without deleting previous full restore while restoring incremental backup.	
check-device	Performs file system check on the backup device.	
format-device	Format the backup device as a preparation step before backup.	

Variable	Description	Default
old-restore <full_int> <increments_int> > domain <domain_str> user <user_str>	<p><full_int> is the full backup version you specify when you configure the backup settings.</p> <p><increments_int> is the number of incremental backups to make between each full backup.</p> <p><domain_str>: optionally specify which domain's mailbox will be restored.</p> <p><user_str>: optionally specify which user's mailbox will be restored.</p> <p>For details, see “system backup-restore-mail” on page 253.</p>	
restore {domain <domain> user <user> host <host>}	<p>Restores mailboxes, or optionally, for the specified domain or user.</p> <p>If you want to restore mailboxes from backups identified by another FQDN, such as a previous FQDN or the FQDN of another FortiMail unit, specify the <host>, which is the FQDN.</p> <p>Usually, you should enter an FQDN of this FortiMail unit, but you may enter the FQDN of another FortiMail unit if you want to import that FortiMail unit's mailbox backup.</p> <p>For example, you may be upgrading to a FortiMail-2000 from a FortiMail-400. Previously, you have used a USB disk to store a backup of the mailboxes of the FortiMail-400, whose fully qualified domain name (FQDN) was fortimail.example.com. You have then configured the FortiMail-2000 to also use the USB disk as its backup media. You could then import the FortiMail-400's mailbox backup to the FortiMail-2000 by entering fortimail.example.com in this field on the FortiMail-2000's web UI.</p>	
start	Initiate an immediate backup. Note that all data on the backup device will be erased.	
stop	Stops any currently running backups.	

Related topics

- [restore config](#)
- [backup](#)
- [debug application burstd](#)

certificate

Use this command to upload and download certificates, and to generate certificate signing requests (CSR).

Syntax

```
execute certificate ca import tftp <file_name> <tftp_ip>
execute certificate ca export tftp <cert_name> <file_name> <tftp_ip>
execute certificate config verify
execute certificate crl import tftp <file_name> <tftp_ip>
execute certificate local export tftp <cert_name> <file_name>
    <tftp_ip>
execute certificate local generate <cert_name> <key_size> <subject>
    <country> <state> <organization> <unit> <email>
execute certificate local import tftp <file_name> <tftp_ip>
execute certificate remote import tftp <file_name> <tftp_ip>
execute certificate remote export tftp <cert_name> <file_name>
    <tftp_ip>
```

Variable	Description	Default
ca import tftp <file_name> <tftp_ip>	Imports the certificate authority (CA) certificate from a TFTP server. Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.	
ca export tftp <cert_name> <file_name> <tftp_ip>	Exports the CA certificate to a TFTP server.	
config verify	Since FortiMail stores configuration information of CA certificates and local certificates in the configuration file and stores the certificates themselves in the file system, in some circumstances (such as a firmware upgrade or an abnormal system shutdown), the certificate configuration and the certificate may be out of sync. Use this command to synchronize the certificate configuration in the configuration file with the certificate in the file system.	
crl import tftp <file_name> <tftp_ip>	Imports the Certificate Revocation List. To ensure that your FortiMail unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses.	
local export tftp <cert_name> <file_name> <tftp_ip>	Exports a certificate signing request or a local certificate to a TFTP server. Note that this command does not support exporting a certificate in PKCS#12 format. To do this, you must go to the web UI.	

Variable	Description	Default
local generate <cert_name> <key_size> <subject> <country> <state> <organization> <unit> <email>	Enter the information required to generate a certificate signing request. Certificate signing request files can then be submitted for verification and signing by a certificate authority (CA).	
local import tftp <file_name> <tftp_ip>	Imports a local certificate from a TFTP server. Note that this command does not support importing a certificate that is in PKCS#12 format. To do this, you must go to the web UI. FortiMail units require a local server certificate that it can present when clients request secure connections, including: <ul style="list-style-type: none"> • the web UI (HTTPS connections only) • webmail (HTTPS connections only) • secure email, such as SMTPS, IMAPS, and POP3S 	
remote import tftp <file_name> <tftp_ip>	Imports the certificate of the online certificate status protocol (OCSP) servers of your certificate authority (CA). OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).	
remote export tftp <cert_name> <file_name> <tftp_ip>	Exports the OCSP certificate to a TFTP server.	

Related topics

- [profile certificate-binding](#)

checklogdisk

Use this command to find and correct errors on the log disk.



Use this command only when recommended by Fortinet Technical Support. Logging is suspended while this command is executing.

Syntax

```
execute checklogdisk
```

Related topics

- [checkmaildisk](#)
- [system top](#)

checkmaildisk

Use this command to find and correct errors on the mail disk. Actions are displayed at the command prompt. If the command cannot fix an error automatically, it displays a list of manual correction options from which you must select.



Use this command only when recommended by Fortinet Technical Support. Email-related functions are suspended while this command is executing.

Syntax

```
execute checkmaildisk
```

Related topics

- [checklogdisk](#)
- [system top](#)

cleanqueue

Select to remove all messages from the deferred queue.

Syntax

```
execute cleanqueue
```

Related topics

- [maintain](#)

create

This is a hidden command. Use this command to create various system-wide, domain-wide, and user-wide antispam settings, such as black/white lists and custom messages.

Syntax

```

execute create blacklist <domain> <blacklist_content>
execute create custom-message <domain> <message_content>
execute create dkim-signing-key
execute create ibe-system-key <content>
execute create resource-share
execute create system-blacklist <content>
execute create system-custom-message <contents>
execute create system-whitelist <content>
execute create system-favicon
execute create user-auto-forward <email_addr> <content>
execute create user-auto-reply <email_addr> <content>
execute create user-blacklist <email_addr> <content>
execute create user-calendar-tag <email_addr> <content>
execute create user-calendar-b64
execute create user-email-tag <email_addr> <content>
execute create user-filter-custom
execute create user-filter-master
execute create user-filter-sieve
execute create user-preference <user_name> <content>
execute create user-primaryaddr <user_name> <content>
execute create user-secondaryaddr <user_name> <content>
execute create user-signature <user_name> <content>
execute create user-whitelist <user_name> <content>
execute create whitelist <domain> <content>

```

Variable	Description	Default
blacklist <domain> <blacklist_content>	Creates domain-wide blacklists. For information about valid formats of the black and white lists, see the <i>FortiMail Administration Guide</i> .	
custom-message <domain> <message_content>	Creates domain-wide custom messages.	
dkim-signing-key	Creates dkim signing key.	
resource-share	Creates a resource share.	
ibe-system-key <content>	Creates IBE system key.	
system-blacklist <content>	Creates system-wide blacklists.	
system-custom-message <contents>	Creates system-wide custom messages.	
system-whitelist <content>	Creates system-wide white lists.	
system-favicon	Creates a system use icon file.	

Variable	Description	Default
user-auto-forward <email_addr> <content>	Creates an auto forward message for a user.	
user-auto-reply <email_addr> <content>	Creates an auto reply message for a user.	
user-blacklist <email_addr> <content>	Creates blacklists for a specific user.	
user-calendar-tag <email_addr> <content>	Creates a user calendar tag.	
user-calendar-base64	Creates a calendar base64 encoded.	
user-email-tag <email_addr> <content>	Creates a user email tag.	
user-filter-custom	Creates a user message filter custom file.	
user-filter-master	Creates a user message filter master file.	
user-filter-sieve	Creates a user message filter sieve file.	
user-preference <user_name> <content>	Configures the user preference settings. For details, see the User chapter in the <i>FortiMail Administration Guide</i> .	
user-primaryaddr <user_name> <content>	Configures the primary email account for the user.	
user-secondaryaddr <user_name> <content>	Configures the secondary email account for the user.	
user-signature <user_name> <content>	Configures the email signature for the user.	
user-whitelist <user_name> <content>	Creates personal whitelists.	
whitelist <domain> <content>	Creates domain-wide whitelists.	

Related topics

- [backup](#)

date

Use this command to set the system date.

Syntax

```
execute date <date_str>
```

Variable	Description	Default
<date_str>	Enter the system date in the format of mm/dd/yyyy.	

Related topics

- [system time manual](#)
- [system time ntp](#)

db

Use this command to repair, rebuild, or reset the following FortiMail databases:

- Address book
- Bayesian database
- Certificate database
- Customized messages
- Dictionaries
- DKIM key database
- Email migration database
- End point database
- End point sender reputation database
- Greylist database
- Greylist exempt database
- IBE database
- Sender reputation database
- User alias database
- User address mapping database

Note: To reset the dictionary database, use “[reset quota](#)” on [page 374](#).

Syntax

```
execute db dump
execute db force-recover
execute db info
execute db rebuild
execute db reset <database>
execute db restore
```

Variable	Description	Default
dump	Dumps one database	
force-recover	Try to repair all of the databases using force recovery.	
info	Provides database information.	

Variable	Description	Default
rebuild	Clean and rebuild all of the databases.	
reset <database>	Clean and rebuild one of the FortiMail databases. <database> is one of the above-listed databases.	
restore	Restores one database.	

Related topics

- [maintain](#)

dlp

Use this command to refresh the DLP fingerprints from the fingerprint server.

Syntax

```
execute dlp refresh <source_name>
```

Variable	Description	Default
<source_name>	Enter the source server address or host name.	

endpoint

Use this command to configure carrier endpoint devices. A carrier end point is any device on the periphery of a carrier's or internet service provider's (ISP) network. It could be, for example, a subscriber's GSM cellular phone, wireless PDA, or computer using DSL service.

Syntax

```
execute endpoint count
execute endpoint data backup tftp <ip_address>
execute endpoint delete <ip_address>
```

Variable	Description	Default
count	Count the total number of endpoint devices in the end point database.	
data backup tftp <ip_address>	Back up the end point database to the specified TFTP server.	
delete <ip_address>	Remove the IP address of an endpoint device from the end point database.	

erase filesystem

Securely erases a file system by filling with random data three times.

Syntax

```
execute erase-filesystem
```

Variable	Description	Default
erase-filesystem		

factoryreset

Use this command to reset the FortiMail unit to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings

This command also erases all the log files and mail data on the hard drive. .



Back up your configuration and mail data before entering this command. This procedure resets all changes that you have made to the FortiMail unit's configuration file and reverts the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the [FortiMail Administration Guide](#).

Syntax

```
execute factoryreset
```

Example

The following example resets the FortiMail unit to default settings for the currently installed firmware version.

```
execute factoryreset
```

The CLI displays the following:

```
This operation will change all settings to  
factory default! Do you want to continue? (y/n)
```

After you enter **y** (yes), the CLI displays the following and logs you out of the CLI:

```
System is resetting to factory default...
```

Related topics

- [restore config](#)
- [backup](#)

factoryreset disk

Use this command to reset the RAID level and partition disk to default settings.

Syntax

```
execute factoryreset disk
```

Related topics

- [backup](#)

fips

Use this command to enable Federal Information Processing Standards-Common Criteria (FIPS-CC) mode.

This enhanced security mode is required by some organizations, but may not be appropriate for others. It is valid only if you have installed a FIPS-certified firmware build. For more information on FIPS, or to obtain a certified build, contact [Fortinet Technical Support](#).

When switching to FIPS mode, you will be prompted to confirm, and must log in again.

To disable FIPS mode, restore the firmware default configuration using [factoryreset](#).



Back up the configuration before enabling FIPS mode. When you enable or disable FIPS-CC mode, all of the existing configuration is lost. For more information on making a complete backup, see the [FortiMail Administration Guide](#).

Syntax

```
execute fips kat {3des | aes | configuration-test | integrity-test |  
                 rng | rsa | sha1-hmac | all}
```

Variable	Description	Default
{3des aes configuration-test integrity-test rng rsa sha1-hmac all}	3des: Triple-DES known answer test. aes: AES known answer test configuration-test: Configuration bypass test. integrity-test: Firmware integrity test. rng: RNG known answer test. rsa: RSA known answer test. sha1-hmac: SHA1-HMAC known answer test. all: All known answer tests.	

Related topics

- [restore image](#)

formatlogdisk

Use this command to reformat the local hard disk that contains log data.



Regularly format the hard disk to improve performance.



Back up all data on the disk before entering this command. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatlogdisk
```

Example

The following example formats the log disk.

```
execute formatlogdisk
```

The CLI displays the following:

```
This operation will erase all data on the log disk!
```

```
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk, Please wait a few seconds!
```

Related topics

- [partitionlogdisk](#)
- [formatmaildisk](#)
- [formatmaildisk_backup](#)

formatmaildisk

Use this command to reformat the local hard disk that contains email data, **without** first performing a backup.

You can alternatively perform a backup before formatting the mail disk. For details, see [“formatmaildisk_backup” on page 330](#).



Regularly format the hard disk to improve performance.



Back up all data on the disk before entering this command. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatmaildisk
```

Example

The following example formats the log disk.

```
execute formatmaildisk
```

The CLI displays the following:

```
This operation will erase all data on the mail disk!  
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk, Please wait a few seconds!
```

Related topics

- [formatmaildisk_backup](#)
- [formatlogdisk](#)

formatmaildisk_backup

Use this command to back up data contained on the mail disk to the log disk, and then format the local mail disk.

You can alternatively format the mail disk without performing a backup. For details, see [“formatmaildisk” on page 329](#).



Regularly format the hard disk to improve performance.

Syntax

```
execute formatmaildisk_backup
```

Related topics

- [formatmaildisk](#)
- [formatlogdisk](#)

forticloud

Use this command to manage the FortiCloud account.

Syntax

```
execute forticloud create
execute forticloud info
execute forticloud join
execute forticloud login
```

Variable	Description	Default
create	Creates a FortiCloud account.	
info	Shows the FortiCloud account info if login in.	
join	Joins an existing FortiCloud account. The device must be added to the account to work.	
login	Logs the user into the FortiCloud account.	

ha commands

Use this command to help debugging FortiMail HA issues.



Type the full command names (such as `ha commands ...`), instead of the abbreviated names (such as `ha com ...`).

Syntax

```
execute ha commands config-sync-start
execute ha commands config-sync-stop
execute ha commands failover-start
execute ha commands failover-stop
```

Variable	Description	Default
config-sync-start	Start synchronizing the HA cluster configuration.	
config-sync-stop	Stop the cluster from completing synchronizing its configuration.	

Variable	Description	Default
failover-start	Allow HA failover to happen.	
failover-stop	Prevent HA failover form happening.	

Related topics

- [cleanqueue](#)

license

Use this command to manage the central management license.

Syntax

```
execute license centrarl-mgmt import tftp <ip> <file_name>
execute license centrarl-mgmt show
```

Variable	Description	Default
import tftp <ip> <file_name>		
show	Display the license information	

ibe data

Use this command to generate and view an IBE data file.

Syntax

```
execute ibe data export-to-file
execute ibe data get-file-info
```

Variable	Description	Default
export-to-file	Generate an IBE data file.	
get-file-info	Get current IBE data file information.	

Related topics

- [db](#)

ibe user

Use this command to maintain the expired users.

Syntax

```
execute ibe user purge-mail <user_name> <level>
execute ibe user clean-expired-user <user_name> <level>
```

Variable	Description	Default
purge-mail <user_name> <level>	Speciy whose mail you want to purge/delete and also specify the verbose level.	
clean-expired-user <user_name> <level>	Specify which user you want to delete and also specify the verbose level.	

Related topics

- [db](#)

lvm

Use this command to control the logical volume manager (LVM) support on the FortiMail-VM platforms.

Since this feature is added in 5.20 release, if you're upgrading from older FortiMail-VM releases to 5.2.0 release, LVM is not enabled by default. If you want to enable it, you must be aware that all the mail data and log data will be erased.

Syntax

```
execute lvm disable
execute lvm enable <percentage>
execute lvm extend <percentage>
execute lvm summary
```

Variable	Description	Default
disable	Stop LVM on the system.	
enable <percentage>	Start LVM on the system. Also specify how much percent of the hard disk space will be allocated to the log disk. The remaining will be assigned to the mail disk. If not specified, the default percentage is 20.	enable (for new install) 20
extend <percentage>	Use this command to add new drives to the system. See above for the usage of percentage.	20
summary	Displays the LVM status and details.	

maintain

Use this command to perform maintenance on mail queues by deleting out-of-date messages.

Syntax

```
execute maintain mailqueue clear age <time_str>
```

Variable	Description	Default
age <time_str>	Enter an age between 1 hour and 10 years. The FortiMail unit deletes mail messages in the mail queues greater than this age. The age consists of an integer appended to a letter that indicates the unit of time: h (hours), d (days), m (months), or y (years).	24h

Example

This example will clear messages that are 23 days old and older.

```
execute maintain mailqueue clear age 23d
```

The CLI would display the following message:

```
Clearing messages in mail queues at least 23 days old.
```

Related topics

- [cleanqueue](#)

nslookup

Use this command to query the DNS server for domain name or IP address mapping or for any other specific DNS record.

Syntax

```
execute nslookup name <fqdn | ip> type <type> class <class> server
<dns_server> port <port_number>
```

Variable	Description	Default
<pre>name <fqdn ip> type <type> class <class> server <dns_server> port <port_number></pre>	<p><fqdn ip>: enter either an IP address or a fully qualified domain name (FQDN) of a host.</p> <p><type>: optionally specify the DNS query type:</p> <ul style="list-style-type: none"> • A -- host address • AAAA -- IPv6 address • ANY -- all cached records • CNAME -- canonical name • DLV -- DNSSEC lookaside validation • DNSKEY -- DNS key • DS -- delegation signer • MX -- mail exchanger • NS -- authoritative name server • NSEC -- next SECure • NSEC3 -- NSEC3 parameters • PTR -- domain name pointer • RRSIG -- DNSSEC signature • SOS -- start of authority zone • SPF -- sender policy framework • TA -- DNSSEC trust authorities • TXT -- text string <p>The default type is A.</p> <p><class>: optionally specify the DNS class type: either IN or ANY.</p> <p><dns_server>: optionally specify the DNS server's host name or IP address. If you do not specify the server here, FortiMail will use its local host DNS settings.</p> <p><port_number>: optionally specify the port number of the DNS server.</p>	<p>A</p> <p>ANY</p> <p>53</p>

Example

You could use this command to determine the DNS resolution for the fully qualified domain name mail.example.com

```
execute nslookup name mail.example.com
```

The CLI would display the following:

```
Name:      example.com
Address: 192.168.1.15
```

Similarly, you could use this command to determine the domain name hosted on the IP address 192.168.1.15:

```
execute nslookup name 192.168.1.15
```

The CLI would display the following:

```
Address: 192.168.1.15
Name:    mail.example.com
```

You could also use this command to determine the host that is mail exchanger (MX) for the domain example.com:

```
execute nslookup name example.com type mx
```

The CLI would display the following:

```
example.com    mail exchanger = 10 mail.example.com.
```

Related topics

- [fortiguard rating](#)
- [ping](#)
- [traceroute](#)
- [system dns](#)

partitionlogdisk

Use this command to adjust the size ratio of the hard disk partitions for log and mail data.



Back up all data on the disks before beginning this procedure. Partitioning the hard disks deletes all files on those disks.

Syntax

```
execute partitionlogdisk <logpercentage_str>
```

Variable	Description	Default
partitionlogdisk <logpercentage_str>	Enter an integer between 10 and 90 to create a partition for log files using that percentage of the total hard disk space. The remaining partition (by default, 75% of the hard disk space) will be used for mail data.	25

Related topics

- [formatlogdisk](#)

ping

Use this command to perform an ICMP ECHO request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by “ping-option” on page 338.

Pings are often used to test connectivity.

Syntax

```
execute ping {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
ping {<fqdn_str> <host_ipv4>}	Enter either the IP address or fully qualified domain name (FQDN) of the host.	

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
 64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
 64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
 64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
 64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
 64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
 5 packets transmitted, 5 packets received, 0% packet loss
 round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between the FortiWeb unit and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds (ms).

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output has been displayed. The administrator halts the ping by pressing Ctrl + C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host may be down, or that there is no route between the FortiMail unit and 10.0.0.1. To determine the cause, further diagnostic tests are required, such as “traceroute” on page 350.

Related topics

- [ping-option](#)
- [smtp-test](#)
- [telnet-test](#)
- [traceroute](#)
- [system dns](#)

ping-option

Use this command to configure behavior of “ping” on page 337.

Syntax

```
execute ping-option data-size <bytes_int>
execute ping-option df-bit {yes | no}
execute ping-option pattern <bufferpattern_hex>
execute ping-option repeat-count <repeat_int>
execute ping-option source {auto | <interface_ipv4>}
execute ping-option timeout <seconds_int>
execute ping-option tos {default | lowcost | lowdelay | reliability |
    throughput}
execute ping-option ttl <hops_int>
execute ping-option validate-reply {yes | no}
execute ping-option view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure <code>pattern <bufferpattern_hex></code> .	56
df-bit {yes no}	Enter either <code>yes</code> to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter <code>no</code> to allow the ICMP packet to be fragmented.	no
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as 00ffaabb, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by <code>data-size <bytes_int></code> .	
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either <code>auto</code> or a FortiMail network interface's IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2

Variable	Description	Default
tos {default lowcost lowdelay reliability throughput}	Enter the IP type-of-service option value, either: <ul style="list-style-type: none"> • default: Do not indicate. (That is, set the TOS byte to 0.) • lowcost: Minimize cost. • lowdelay: Minimize delay. • reliability: Maximize reliability. • throughput: Maximize throughput. 	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	

Example

This example sets the number of pings to three and the source IP address to that of the port2 network interface, 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
  Repeat Count: 3
  Data Size: 56
  Timeout: 2
  TTL: 64
  TOS: 0
  DF bit: unset
  Source Address: 10.10.10.1
  Pattern:
  Pattern Size in Bytes: 0
  Validate Reply: no
```

Related topics

- [ping](#)
- [traceroute](#)

ping6

Use this command to perform a ping6 request to an IPv6 host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by “[ping6-option](#)” on [page 340](#).

Pings are often used to test connectivity.

Syntax

```
execute ping6 {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
ping6 {<fqdn_str> <host_ipv4>}	Enter either the IP address or fully qualified domain name (FQDN) of the host.	

Related topics

- ping
- ping6-option

ping6-option

Use this command to configure behavior of “ping6” on page 339.

Syntax

```
execute ping6-option data-size <bytes_int>
execute ping6-option pattern <bufferpattern_hex>
execute ping6-option repeat-count <repeat_int>
execute ping6-option source {auto | <interface_ipv4>}
execute ping6-option timeout <seconds_int>
execute ping6-option tos {default | lowcost | lowdelay | reliability
    | throughput}
execute ping6-option ttl <hops_int>
execute ping6-option validate-reply {yes | no}
execute ping6-option view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure <code>pattern <bufferpattern_hex></code> .	56
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as 00ffaabb, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by <code>data-size <bytes_int></code> .	
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either <code>auto</code> or a FortiMail network interface's IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2

Variable	Description	Default
tos {default lowcost lowdelay reliability throughput}	Enter the IP type-of-service option value, either: <ul style="list-style-type: none"> • default: Do not indicate. (That is, set the TOS byte to 0.) • lowcost: Minimize cost. • lowdelay: Minimize delay. • reliability: Maximize reliability. • throughput: Maximize throughput. 	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	

Related topics

- [ping](#)
- [ping6](#)

raid

Use this command to find and add a hard disk to the array unit after you insert a second hard disk into the drive bay. .



This command is only available for some FortiMail platforms which support RAID.

Syntax

```
execute raid add-disk
```

Example

You could notify the RAID controller to add the hard disk to the array unit after inserting a new hard disk.

```
execute raid
```

The CLI displays the following:

```
This operation will scan for new hard drives and add them into the RAID
array
```

```
Do you want to continue? (y/n)
```

After you enter *y* (yes), if all hard disks have already been added to an array, the CLI displays the following:

```
existing raid disk at 12 is 120034123776
existing raid disk at 13 is 120034123776
no NEW disks in the system
```

Related topics

- [system status](#)

reboot

Use this command to restart the FortiMail unit.

Syntax

```
execute reboot
```

Example

The following example reboots the FortiMail unit.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !  
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

Related topics

- [shutdown](#)

reload

If you set your console to batch mode, use this command to flush the current configuration from system memory (RAM) and reload the configuration from a previously saved configuration file.

In addition, you can also use this command to reload individual daemons that have crashed. In this case, the command is as following:

```
exec reload [{httpd | ...}]
```

where `[{httpd | ...}]` indicates the name of a specific daemon that you want to restart, if you want to limit the reload to a specific daemon.

For example, if HTTP and HTTPS access are enabled, but you cannot get a connection response on webmail or the GUI, although you can still connect via SSH and ping. Thus you

know that the FortiMail unit has not crashed entirely. If you do not want to reboot because this would interrupt SMTP, you can choose to restart the HTTP daemon only.

```
FortiMail-400 # exec reload httpd
Restart httpd?
Do you want to continue? (y/n)y
```

```
Reloading httpd....done
```

Note that the command does not check whether your indicated daemon actually exists. It simply indicates whether the command is executed. If the command does not take a few seconds to execute, it is possible that the daemon does not really exist.

Syntax

```
execute reload [<daemon_name>]
```

Related topics

- [reboot](#)
- [restore config](#)
- [restore image](#)
- [debug application cmdb_event](#)
- [system top](#)

restore as

Use this command to restore an antispam configuration file from a TFTP server.

Syntax

```
execute restore as tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

Related topics

- [restore av](#)

restore av

use this command to restore an antivirus configuration file from a TFTP server.

Syntax

```
execute restore av tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

Related topics

- [restore as](#)

restore config

Use this command to restore a primary configuration file from a TFTP server.



Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the [FortiMail Administration Guide](#).



Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiMail unit to its firmware/factory default configuration. For information on installing firmware via TFTP boot interrupt, see the [FortiMail Administration Guide](#).

Syntax

```
execute restore config {tftp <filename_str> <server_ipv4> |  
management-station {normal | template} <revision_int>}
```

Variable	Description	Default
<filename_str>	If you want to restore a configuration file stored on a TFTP server, enter the name of the configuration file.	
<server_ipv4>	If you want to restore a configuration file stored on a TFTP server, enter the IP address of the TFTP server.	

Variable	Description	Default
management-station {normal template}	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the management-station keyword then enter either: <ul style="list-style-type: none"> normal: Restore a configuration revision number. template: Apply a template revision number. 	
<revision_int>	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the revision number of the configuration file or template.	

Example

This example restores configuration file revision 2, which is stored on the FortiManager unit.

```
execute restore config management-station normal 2
```

The CLI displays the following:

This operation will overwrite the current settings!

Do you want to continue? (y/n)

After you enter **y** (yes), the CLI displays the following:

```
Connect to FortiManager ...
```

```
Please wait...
```

Example

This example restores a configuration file from a TFTP server at 172.16.1.5.

```
execute restore config tftp fml.cfg 172.16.1.5
```

The CLI displays the following:

This operation will overwrite the current settings!

(The current admin password will be preserved.)

Do you want to continue? (y/n)

After you enter **y** (yes), the CLI displays the following, then terminates the SSH connection and reboots with the restored configuration:

```
Connect to tftp server 172.16.1.5 ...
```

```
Please wait...
```

```
Get config file from tftp server OK.
```

```
File check OK.
```

Related topics

- [backup](#)
- [system central-management](#)

restore image

Use this command to restore a firmware file from a TFTP server or FortiManager unit.



Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the [FortiMail Administration Guide](#).

Syntax

```
execute restore image {tftp <filename_str> <server_ipv4> |  
management-station <image_id>}
```

Variable	Description	Default
<filename_str>	If you want to restore a firmware file stored on a TFTP server, enter the name of the firmware file backup file.	
<server_ipv4>	If you want to restore a firmware file stored on a TFTP server, enter the IP address of the TFTP server.	
management-station <image_id>	If you want to restore a firmware file stored on a FortiManager unit, enter the management-station keyword then enter the ID number of the firmware file.	

Example

This example restores firmware file FE_2000A-v300-build397-FORTINET.out, which is stored on the TFTP server 192.168.1.20.

```
execute restore image tftp FE_2000A-v300-build397-FORTINET.out  
192.168.1.20
```

The CLI displays the following:

```
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
```

After you enter **y** (yes), the CLI displays the following:

```
Connect to tftp server 192.168.1.20 ...  
Please wait...  
#####  
Get image from tftp server OK.  
Check image OK.
```

Related topics

- [restore config](#)
- [system central-management](#)

restore mail-queues

Use this command to restore a mail queue file from a TFTP server.



Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit’s configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the [FortiMail Administration Guide](#).

Syntax

```
execute restore mail-queues {tftp <filename_str> <server_ipv4>}
```

Variable	Description	Default
<filename_str>	If you want to restore a firmware file stored on a TFTP server, enter the name of the firmware file backup file.	
<server_ipv4>	If you want to restore a firmware file stored on a TFTP server, enter the IP address of the TFTP server.	

Related topics

- [restore config](#)

sched-backup

Use this command to schedule backup to FortiManager.

Syntax

```
execute sched-backup
```

shutdown

Use this command to prepare the FortiMail unit to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.



Power off the FortiMail unit only after issuing this command. Unplugging or switching off the FortiMail unit without issuing this command could result in data loss.

Syntax

```
execute shutdown
```

Example

The following example halts the FortiMail unit.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

Related topics

- [reboot](#)

smtptest

Use this command to test SMTP connectivity to a specified host.

Syntax

```
execute smtptest {<fqdn_str> | <host_ipv4>}[:<port_int>] [domain
<domain_str>]
```

Variable	Description	Default
{<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	No default.
[:<port_int>]	If the SMTP server listens on a port number other than port 25, enter a colon (:) followed by the port number.	:25
[domain <domain_str>]	If you want to test the connection from an IP address in the protected domain's IP pool, enter the name of the protected domain.	No default.

Example

This example tests the connection to an SMTP server at 192.168.1.10 on port 2525. For the outgoing connection, the FortiMail unit uses the source IP address 192.168.1.20 from the IP pool selected in the protected domain example.com.

```
execute smtptest 192.168.1.10:2525 domain example.com
```

The CLI displays the following:

(using 192.168.1.20 to connect)

Remote Output:

```
220 fortimail.example.com ESMTP Smtpd; Mon, 19 Jan 2009
13:27:35 -0500
```

Connection Status:

```
Connecting to remote host succeeded.
```

Related topics

- [telnettest](#)
- [traceroute](#)
- [ping](#)
- [system dns](#)

ssh

Use this command to connect to another device via SSH.

Syntax

```
execute ssh <username@host> <password>
```

Variable	Description	Default
<username@host> <password>	Enter the user name and password. The host can be an IP address or the host name of the remote device.	

storage

Use this command to configure remote file storage.

Syntax

```
execute storage format
execute storage fscheck
execute storage start
execute storage test
```

Variable	Description	Default
format	Remove all data on the remote storage device.	
fscheck	Check the remote file storage system.	
start	Start the remote storage daemon.	
test	Test the remote file storage system.	

telnettest

Use this command to test Telnet connectivity to a specified host.

Syntax

```
execute telnettest {<fqdn_str> | <host_ipv4>}[:<port_int>]
```

Variable	Description	Default
{<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the Telnet server.	No default.
[:<port_int>]	If the Telnet server listens on a port number other than port 23, enter a colon (:) followed by the port number.	:23

Example

This example tests the connection to an Telnet server at 192.168.1.10 on port 2323.

```
execute telnettest 192.168.1.10:2323
```

The CLI displays the following:

(using 192.168.1.20 to connect)

Remote Output(hex):

```
FF FD 18 FF FD 20 FF FD
23 FF FD 27
```

Connection Status:

```
Connecting to remote host succeeded.
```

Related topics

- [smtptest](#)
- [traceroute](#)
- [ping](#)
- [system dns](#)

traceroute

Use this command to use ICMP to test the connection between the FortiMail unit and another network device, and display information about the time required for network hops between the device and the FortiMail unit.

Syntax

```
execute traceroute {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
traceroute {<fqdn_str> <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the host.	No default.

Example

This example tests connectivity between the FortiMail unit and <http://docs.fortinet.com>. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiMail# execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte
  packets
 1  172.16.1.200 (172.16.1.200)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
 1 172.16.1.2  0 ms  0 ms  0 ms
 2 10.10.10.1 <static.isp.example.net>  2 ms  1 ms  2 ms
 3 10.20.20.1  1 ms  5 ms  1 ms
 4 10.10.10.2 <core.isp.example.net> 171 ms 186 ms 14 ms
 5 10.30.30.1 <isp2.example.net> 10 ms 11 ms 10 ms
 6 10.40.40.1 73 ms 74 ms 75 ms
 7 192.168.1.1 79 ms 77 ms 79 ms
 8 192.168.1.2 73 ms 73 ms 79 ms
 9 192.168.1.10 73 ms 73 ms 79 ms
10 192.168.1.10 73 ms 73 ms 79 ms
```

Example

This example attempts to test connectivity between the FortiMail unit and example.com. However, the FortiMail unit could not trace the route, because the primary or secondary DNS server that the FortiMail unit is configured to query could not resolve the FQDN example.com into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiMail# execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiMail unit with the IP addresses of DNS servers that are able to resolve the FQDN example.com. For details, see “[system dns](#)” on [page 262](#).

Related topics

- [smtptest](#)
- [telnettest](#)
- [ping](#)
- [ping-option](#)
- [system dns](#)

update

Use this command to manually request updates to the FortiGuard Antivirus and FortiGuard Antispam engine and definitions from the FortiGuard Distribution Network (FDN).

You can alternatively or additionally configure scheduled updates and push updates. For details, see “system fortiguard antivirus” on page 267 and “system fortiguard antispam” on page 269.

Syntax

```
execute update {as | av | now}
```

Related topics

- [system fortiguard antivirus](#)
- [system fortiguard antispam](#)
- [debug application updated](#)

user-config

Use this command to generate a file with the latest user-specific configurations, such as user preferences, personal black/white lists, and secondary addresses, to the user configuration file, so that you will have the latest configuration when you make a configuration backup using backup.

Syntax

```
execute user-config generate
execute user-config getinfo
```

Variable	Description	Default
generate	Updates the user configuration file with the latest user-specific configuration.	
getinfo	Displays the timestamp when the last configuration file update was performed.	

Related topics

- [backup](#)

vm

Use this command to upload a VM license.

Syntax

```
execute vm license tftp <license_file_name> <tftp_server_ip>
```


Variable	Description	Default
<license_file_name> <tftp_server_ip>	Specify the license file name and the TFTP server IP address.	

get

`get` commands display a part of your FortiMail unit's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays **all** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
FortiMail# get system dns

primary          : 172.16.95.19
secondary        : 0.0.0.0
private-ip-query : enable
cache            : enable
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has been reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
FortiMail# get system dns
```

and this command would not:

```
FortiMail# get
```

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding config commands in the `config` chapter.

Other `get` commands, such as `system performance`, are used to display system information that is **not** configurable. This chapter describes this type of `get` command.

This chapter describes the following commands.

`system performance`

`system status`



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` & `show full-configuration` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see “`config`” on page 27.

system performance

Displays the FortiMail unit's CPU usage, memory usage, system load, and up time.

Syntax

```
get system performance
```

Example

```
FortiMail# get system performance
CPU usage:      0% used, 100% idle
Memory usage:   17% used
System Load:    5
Uptime:         0 days,  8 hours,  24 minutes.
```

Related topics

- [system status](#)

system status

Use this command to display FortiMail system status information including:

- firmware version, build number and date
- antivirus definition version and release date and time
- FortiMail unit serial number and BIOS version
- log hard disk availability
- mailbox disk availability
- host name
- operation mode
- distribution scope
- branching point (same as firmware build number)
- release version
- system time

Syntax

```
get system status
```

Example

```
FortiMail-400 # get system status
Version: FortiMail-400 v4.0.0,build0087,091105
Virus-DB: 11.23(11/05/2009 01:20)
Serial-Number: FE-4002905500226
BIOS version: 04000000
Log disk: Capacity 20 GB, Used 1 GB ( 8.27%), Free 18 GB
Mailbox disk: Capacity 89 GB, Used 278 MB ( 0.31%) , Free 89 GB
Hostname: FortiMail-400
Operation Mode: Transparent
Distribution: International
Branch point: 087
Release Version Information: v4.0.0
System time: Thu Nov  5 16:25:31 2009
```

Related topics

- [system performance](#)

show & show full-configuration

The `show` commands display a part of your FortiMail unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see the `config` chapters.

Unlike `get`, `show` does **not** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
FortiMail# show system dns
config system dns
    set primary 172.16.1.10
end
```

Notice that the command does **not** display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.

Exceptions include `show full-configuration` commands. This displays the full configuration, **including** the default settings, similar to `get` commands. However, `show full-configuration` output uses configuration file syntax, while `get` commands do not.

For example, you might show the current DNS settings, **including** settings that remain at their default values (differences highlighted in bold):

```
FortiMail# show full-configuration system dns
config system dns
    set primary 172.16.1.10
    set secondary 172.16.1.11
    set private-ip-query disable
    set cache enable
end
```

Depending on whether or not you have specified an object, like `get`, `show` may display one of two different outputs: either the configuration that you have just entered but not yet saved, or the configuration as it currently exists on the disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `show` displays two different outputs (differences highlighted in bold):

```
FortiMail# config system dns
FortiMail (dns)# set secondary 192.168.1.10
FortiMail (dns)# show
config system dns
    set primary 172.16.1.10
    set secondary 192.168.1.10
end
FortiMail (dns)# show system dns
config system dns
    set primary 172.16.1.10
end
```

The first output from `show` indicates the value that you have configured but not yet saved; the second output from `show` indicates the value that was last saved to disk.



If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `show`, with and without the object name, can be a useful way to remind yourself.

Index

Numerics

501 240
550 105, 154, 156, 161, 177, 178

A

abort 18
access control
 authentication 155
 default action 153
 rules 229
access controls 19
ACL 153
action
 default 153
address map
 LDAP 211
admin 9
administrative access protocol 285
alert email
 event categories 140
 recipients 139
alias 216
ambiguous command 13, 24
antispam
 log messages 137, 138
antivirus
 log messages 137, 138
 profile 104, 176
 scan 105, 179
ASCII 25, 203
attachment 113, 188, 193
AUTH 153
authentication 110, 183
 administrator 250
 certificate vs. password 96, 164
 LDAP 211
 profile 110, 183
 SMTP 110, 153, 183

B

batch changes 8, 25
baud rate 25
bind DN 217
bits per second (bps) 9
blind carbon copy (BCC) 175, 181, 201
boot interrupt 8, 344
bypass
 antispam scan 154

C

carrier 39
 end point 30, 31

cellular phone 39
certificate
 binding profile 187
 personal 96, 164
 server 257, 273, 321
certificate authority (CA) 256, 258, 313, 320, 321
certificate revocation list (CRL) 256, 258, 313, 320, 321
characters, special 24
CIDR 15
CLI
 connecting 8
 connecting to the 8
command 13
 abbreviation 24
 ambiguous 13, 24
 completion 23
 help 23
 incomplete 13
 interactive 24
 prompt 16, 23
 scope 13, 14
command line interface (CLI) 13
comma-separated value (CSV) 135
config router 357
configuration script 8
connecting to the FortiMail CLI using SSH 11
connecting to the FortiMail CLI using Telnet 12
connecting to the FortiMail console 8
console port 8, 9
content
 profile 113, 188
Content-Type 121, 198
CPU usage 354
CRAM-MD5 146

D

DATA 153
DB-9 8
default
 action 153
 administrator account 9
 password 9
definitions 13
delay period
 greylist 41
delete, shell command 17
delivery rules 229
delivery status notification (DSN) 209, 242, 295
dictionary profile 203
 dictionary group 208
DIGEST-MD5 146
digital certificate requests 256, 257, 258

- digital subscriber line (DSL) 39
- discard 105, 154, 177, 178, 200
- disclaimer 260
- disk space
 - quota 130
 - user account 130
- document type definition (DTD) 121, 198
- domain
 - query 219
- dotted decimal 15
- dynamic IP address 39

E

- edit
 - shell command 17
- _email 15
- email access
 - configuring 153
- email address group 208
- encoding 25
- encryption
 - profile 209
- end
 - command in an edit shell 18
 - shell command 17
- end of message (EOM) 235
- error message 14
- escape sequence 24
- expected input 13
- extended simple mail transport (ESMTP) 146

F

- failover 280, 282
- Federal Information Processing Standards-Common Criteria (FIPS-CC) 328
- field 14
- file type 117, 193
- Firefox 276
- firmware
 - restoring 8
- flow control 9
- font 25
- FortiAnalyzer 134
- FortiGuard
 - Antivirus 267
- FortiGuard Distribution Server (FDS) 267, 270
- Fortinet
 - Technical Support 328
- _fqdn 15
- fully qualified domain name (FQDN) 15

G

- gateway mode 288
- get
 - edit shell command 18
 - shell command 18

- greylist
 - delay period 41
 - window 41
- group
 - LDAP 165
- GSM 39

H

- HA
 - and NAS 283
 - failover 280, 282
 - wait for recovery then assume slave role 284
 - wait for recovery then restore original role 284
- heuristic scan
 - antivirus 178
- high availability (HA) 276
- history log 235
- HTTP
 - webmail access 110, 183
- HTTPS 110, 183, 257, 321
- hypertext markup language (HTML) 121, 197

I

- IBE
 - log messages 138
- identity-based encryption (IBE) 158
- IMAP
 - secure 257, 321
- incomplete command 13
- indentation 14
- _index 15
- index number 15
- input constraints 13
- _int 15
- interface address
 - resetting 327, 344, 346, 347
- International characters 25
- Internet Explorer 276
- Internet service provider (ISP) 39, 145
- IP address group 210
- IP pool 85
- IP-based policy 110, 183
- _ipv4 15
- _ipv4/mask 15
- _ipv4mask 15
- _ipv4range 15
- _ipv6 15
- _ipv6mask 15
- iSCSI 151, 254
- iso-8859-1 204, 205, 206

K

- key 11

L

- language 25
 - web-based manager 252
- Layer 2 bridge 287, 288

LDAP

- address map 211
- bind 217
- bind DN 217
- cache 217
- profile 211
- query 219
- query string 215, 216
- secure connection 223
- timeout 224
- TTL 217

LDAPS 223

- line endings 26
- local console access 8
- log
 - FortiAnalyzer 134
 - Syslog 134
- LOGIN 146
- login prompt 9

M

- MAIL FROM 85, 153, 159, 162, 165, 237
- mailbox
 - restoration 319
 - spam 102, 108, 128, 175, 181
- maximum message size 86
- maximum transportation unit (MTU) 285
- memory usage 354
- Microsoft Active Directory 223
- mobile phone 39
- monospace 121, 198
- MTA
 - log messages 136, 138
- multipart/alternative 121, 198
- MX record 144

N

- _name 15
- Netscape 276
- network area storage (NAS)
 - server 283
- network file storage (NFS) 150
- network file system (NFS) 151, 254
- network time protocol (NTP) 307
- next 19
- no object in the end 13
- null modem 9, 10

O

- object 13
- objectClass 215, 216
- on HA failure
 - wait for recovery then assume slave role 284
 - wait for recovery then restore original role 284
- Online Certificate Status Protocol (OCSP)
 - 258, 313, 315, 321
- open relay 153
- option 14
- outgoing proxy 144

P

- parity 9
- password 9, 96, 164
- _pattern 15
- pattern 15
- peer connection 9
- permissions 19
- personal digital assistant (PDA) 39
- phone 39
- PKI user 313
- PLAIN 146
- plain text 121, 198
- plain text editor 25
- policy
 - domain associations 133
 - IP-based 110, 183
- POP3 295
 - secure 257, 321
- port number 296
- profile
 - antivirus 104, 176
 - certificate binding 187
 - content 113, 188
 - dictionary 203
 - encryption 209
 - LDAP 211
 - session 229
- proxy
 - log messages 136, 138
- proxyAddresses 215
- PTR record 263
- public key infrastructure (PKI) 313
- purge, shell command 18

Q

- quarantine
 - per-recipient 164
 - release via email 102
 - release via web 103
- query
 - filter 215, 216, 219
 - for user group 165
 - LDAP 219
 - reverse DNS 156
 - SMTP 91
- quota 130

R

- rate limit 233
- RCPT TO 98, 144, 153, 158, 159, 165, 236, 237, 238
- Received 237
- recipient address rewrite
 - 101, 103, 107, 109, 127, 129, 174, 176, 180, 182, 200, 201, 202
- recipient address verification 91
- recipient-based policy
 - incoming 110, 183
- regular expression 15, 155, 156, 157, 204, 205, 206
- regular expression (regex) 32

- reject 105, 154, 161, 177, 178
- relay 154
 - access denied 154
 - log messages 136, 138
- Relaying denied 154, 156
- remote authentication dial-in user service (RADIUS)
 - 110, 183
 - and endpoint reputation 234
- rename, shell command 18
- replacement messages
 - custom 50
- reserved characters 24
- restoring the firmware 8
- reverse DNS 156
- RFC
 - 2476 296
 - 2821 31, 91, 297
 - 2822 102, 108, 128, 175, 181, 202
 - 822 216
- rfc822MailMember 216
- RJ-45 8, 10
- RJ-45-to-DB-9 9, 10

S

- secure MIME (S/MIME) 187, 209
- Secure Shell (SSH)
 - key 11
- secure shell (SSH) 254
- secure SMTP 296
- sender identity, different 162
- serial communications (COM) port 9, 10
- server mode 110, 183, 288
- session
 - profile 229
 - SMTP 153
- set 19
- setting administrative access for SSH or Telnet 9
- share 254
- shell command
 - delete 17
 - edit 17
 - end 17
 - get 18
 - purge 18
 - rename 18
 - show 18
- show 19
- show, shell command 18
- simple network management protocol (SNMP) 50, 301
- SMB 254

SMTP

- AUTH 146, 153
- DATA 153
- discard 105, 154, 177, 178, 200
- greeting 240
- MAIL FROM 153
- proxy 154
- RCPT TO 153
- reject 154
- relay 154
- reply code 501 240
- reply code 550 105, 154, 156, 161, 177, 178
- server authentication 110, 183
- session 229
- STARTTLS 153, 296
- VERFY 91

SMTPS

- 86, 146, 257, 296, 321

- special characters 24, 25
- SSH 8, 9, 10, 11
 - key 11
- SSL 146, 223, 296
- STARTTLS 153
- _str 15
- string 15
- strong encryption 276
- sub-command 13, 14, 16, 17
- subject line 113, 188, 203
- subscriber ID 235
- syntax 13
- Syslog 134

T

- table 13
- Telnet 8, 9, 12
- temporary failure 161
- text/html 121, 198
- time to live (TTL)
 - greylist 41
- timeout 224
- tips and tricks 23
- TLS 146, 296
- top level domain (TLD) 156
- transparent mode 162, 287, 288
- transport layer security (TLS) 256

U

- uniform resource identifier (URI) 15
- uniform resource locator (URL) 15
- unknown action 13
- unset 19
- up time 354
- _url 15
- US-ASCII 25
- USB 319

- user
 - account 110, 183
 - group 211
 - name 96, 164
 - PKI 313
 - preferences 103
 - quota 130
- User Principle Name (UPN) 217
- using the CLI 8
- UTF-8 25, 203, 204, 205, 206

V

- _v4mask 15
- _v6mask 15
- value 14
- value parse error 14, 15
- viruses
 - scan for 105, 179
- VERFY 91

W

- wait for recovery then assume slave role
 - on HA failure 284
- wait for recovery then restore original role
 - on HA failure 284
- web-based manager
 - language 252
- webmail
 - access 110, 183
 - disk space 130
 - password 223
 - white list 103
- white list
 - personal 103
- wild cards 15, 168
- Windows share 254

X

- X-Content-Filter 202
- X-Custom-Header 102, 108, 128, 175, 181
- X-FEAS-ATTACHMENT-FILTER 121, 197

